Издательство «Знание»

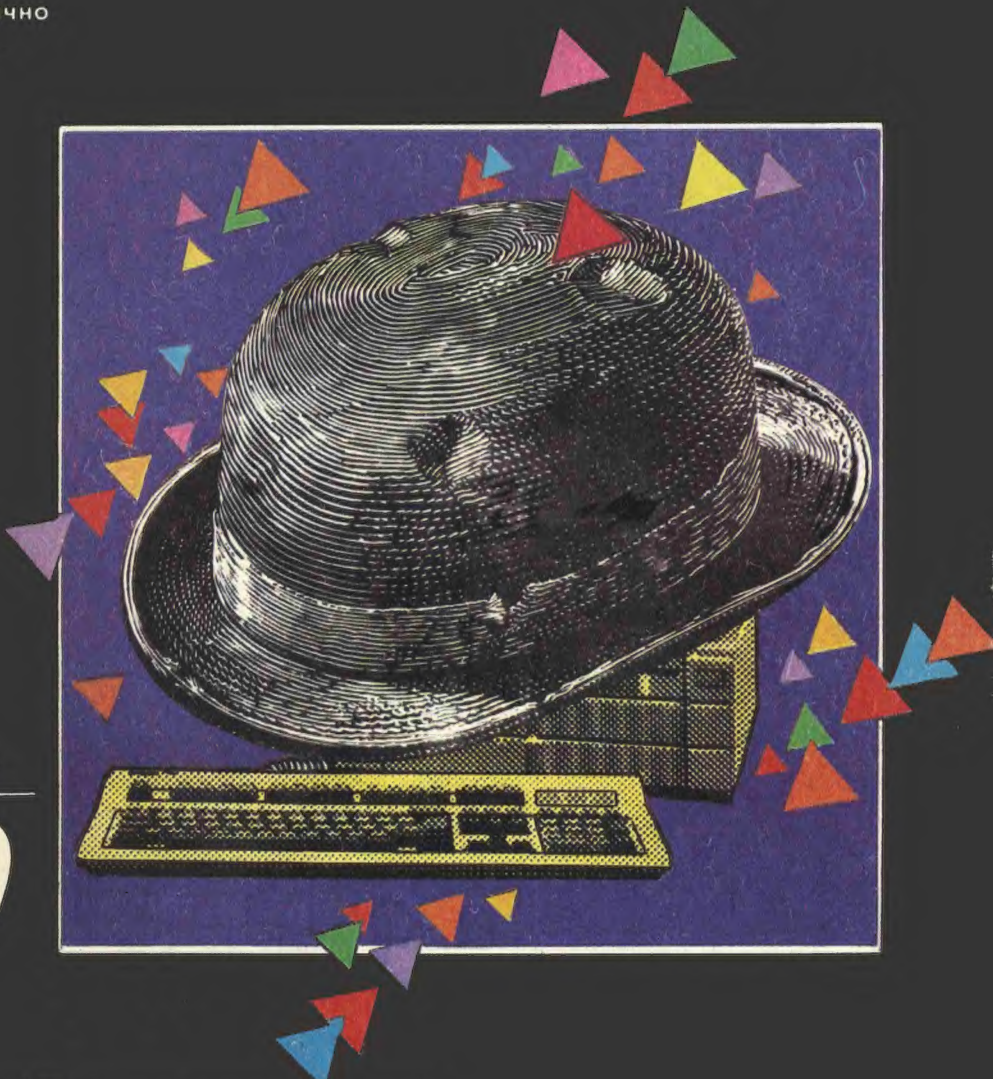
ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ЕЁ ПРИМЕНЕНИЕ

Новое в жизни, науке, технике

Подписная научно-популярная серия

Издается ежемесячно с 1988 г.

Защита информации



1990

9

Новое
в жизни,
науке,
технике

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ЕЁ ПРИМЕНЕНИЕ

Подписная
научно-
популярная
серия

9/1990

Издается
ежемесячно
с 1988 г.

ЗАЩИТА ИНФОРМАЦИИ

В номере:

В.В.Голубев, П.А.Дубров, Г.А.Павлов
КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ И ЗАЩИТА ИНФОРМАЦИИ

РУБРИКИ

Переводы
БК за рога
Терминал. Компьютерный клуб школьников

Издательство
"Знание"
Москва
1990

ББК 32.97
З-40

Авторы выпуска

ГОЛУБЕВ Владимир Владимирович — старший научный сотрудник Военной академии им. Ф.Э.Дзержинского, программист.

ДУБРОВ Павел Александрович — младший научный сотрудник Военной академии им. Ф.Э.Дзержинского, программист.

ПАВЛОВ Геннадий Алексеевич — кандидат технических наук, доцент.

СУЯРГУЛОВ Марат Латыпович — программист.

УТЕНКОВ Сергей Альбертович — инженер, журналист.

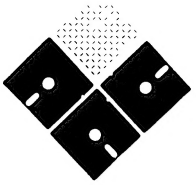
ПЕРЕХОД Игорь Александрович — кандидат физико-математических наук, доцент Симферопольского государственного университета.

НАДЕЖИН Алексей Михайлович — оператор ЭВМ, программист.

РЕДАКТОР Б.М.ВАСИЛЬЕВ

ISBN 5-07-001511-7

© Издательство "Знание", 1990 г.



Здесь рассмотрены лишь некоторые аспекты многогранной проблемы защиты информации в ВС. Более подробно изложены задачи аутентификации пользователей, защиты паролей, защиты от компьютерных вирусов. Заинтересованные читатели могут обратиться к специальным выпускам журналов "ТИИЭР" [6] и "Зарубежная радиоэлектроника" [11], содержащим обширный материал по вышеназванным проблемам. Там же указан ряд монографий, переведенных на русский язык.

В.В.Голубев,
П.А.Дубров,
Г.А.Павлов

Компьютерные преступления и защита информации в вычислительных системах

В последнее время проблемы, связанные с защитой информации, привлекают все большее внимание как специалистов в области компьютерной безопасности, так и многочисленных рядовых пользователей вычислительных систем. Это связано с глубокими изменениями, вносимыми компьютерной технологией в нашу жизнь.

Изменился сам подход к понятию "информация". Этот термин все чаще используется для обозначения специального товара, который можно купить, продать, обменять на что-то другое и т.д. При этом стоимость подобного товара зачастую превосходит в десятки, а то и в сотни раз стоимость самой вычислительной системы, в рамках которой он функционирует.

Естественно, возникает потребность защитить информацию от несанкционированного доступа, кражи, уничтожения и других преступных действий. Отдельно встает вопрос о защите авторских прав на информационные продукты: программы, алгоритмы, данные, результаты.

Авторы вполне отдают себе отчет в том, насколько сложной и комплексной является затронутая ими проблема. Поэтому, отнюдь не претендуя на полноту изложения материала, авторы попытались осветить причины, побуждающие защищать информацию, находящуюся в вычислительной системе: действия, способные исказить и уничтожить информацию, методы защиты информации.

Если читатель почерпнет в статье сведения, достаточные для практического повышения безопасности вычислительных систем, авторы сочтут свою цель вполне достигнутой.

Компьютерные преступления вчера и сегодня

Компактные, сравнительно недорогие, снабженные "дружественным" программным обеспечением, персональные ЭВМ представляют собой основу создания разветвленной информационной инфраструктуры, включающей банки данных и сети ЭВМ. Ставший реальностью нашего времени "информационный взрыв" обусловливает растущий интерес к ПК во всем мире. Если к концу 1987 г. в США насчитывалось более 30 млн. ПК, то в 1990 г. количество ПК в этой стране приблизится к количеству установленных телефонных аппаратов [1]. В СССР функционирует около 300 тыс. ПК, хотя потенциальный рынок готов поглотить и 22 млн.

К сожалению, вместе с ростом числа компьютеров возросла зависимость и уязвимость человеческого общества от разнообразных компьютерных систем. Во многих странах на них возложены обязанности по сбору налогов, переписи населения, обеспечению страхования и медицинского обслуживания, электронной оплате сделок, управлению транспортом и авиацией. Особую роль эти системы играют в военной области.

На некоторой стадии эволюции ЭВМ стали притягательной силой для организованных преступных групп и преступников-одиночек, владеющих необходимыми средствами для совершения крупномасштабных мошен-

нических операций, проведения диверсий, саботажа, хищения секретной информации. Возникла острая необходимость в защите общества от подобных действий. Силы правопорядка, юристы, криминологи, специалисты в области национальной безопасности столкнулись с совершенно новой, неожиданной проблемой. События не заставили себя долго ждать...

В 1971 г американская железнодорожная компания "Нью-Йорк Пенн Централ Рейлроуд" обнаружила пропажу 200 принадлежащих ей вагонов с ценными грузами. При проверке выяснилось, что подобная участь постигла вагоны и ряда других транспортных фирм. Стоимость отдельных вагонов превышала 60 тыс. долл. Тщательно проведенное расследование позволило установить, что в ЭВМ, управляющую процессом адресации вагонов, были введены заведомо неправильные данные. Федеральный суд присяжных пришел к выводу, что это дело рук преступной организации, укравшей таким образом товаров на несколько миллионов долл. [2].

1972 год. В Калифорнии разоблачен некий студент машиностроительного института, который похитил у известной телефонной компании более 1 млн. долл., пользуясь только телефонным аппаратом. Зная секретный пароль, обеспечивающий доступ к главной ЭВМ фирмы, студент размещал с выгодой для себя различные заказы. Суд приговорил мошенника к 60 дням тюремного заключения и 3 годам условно. Впоследствии он стал преуспевающим консультантом в области компьютерной безопасности, указывая владельцам компаний на возможные пути несанционированного доступа к их ЭВМ [2].

Проходит всего год, и новое компьютерное преступление становится главной сенсацией США. В крупнейшем фонде страны — фонде Справедливости оказались подделаны страховые полисы на сумму примерно 2 млрд.долл. Подвергая данные в ЭВМ фальсификации, руководству фонда удавалось в течение длительного периода времени поддерживать миф о его полном финансовом благополучии. Десятки фирм, вкладывавшие средства в этот фонд, оказались введены в заблуждение, некоторые из них обанкротились [3].

Список подобных дел можно многократно продолжить — преступления, совершаемые с помощью ЭВМ, стали горькой реальностью. Четкого определения компьютерных преступлений не существует. Некоторые специалисты относят к ним использование ЭВМ в целях хищения крупных денежных сумм, другие добавляют к этому и незаконное пользование услугами, посягательство на личную и государственную тайны, хищение информации, акты терроризма и вмешательства в ответственные системы управления и многое другое. Так или иначе в этих преступлениях всегда замешан компьютер: либо как инструментарий преступника, либо как его цель.

Анализ множества компьютерных преступлений позволяет описать "среднего" преступника следующим образом. Это молодой (около 35 лет) человек, отлично разбирающийся в вычислительной технике, виртуозно владеющий программированием. Зачастую он совершает преступление, не преследуя при этом прямых материальных выгод. Для него могут быть важнее другие мотивы: утвердить свое "я", отомстить за обиду, просто "пошутить".

Подобные преступления очень трудно раскрываются — достаточно стереть программу из памяти ЭВМ, и его следы исчезают. В случае же если программа обнаружена — как доказать ее авторство? Не удивительно, что суды крайне неохотно принимают подобные дела к производству.

Опубликованный недавно в США отчет национального центра компьютерной безопасности позволяет получить некоторое представление о размахе преступлений, совершаемых с помощью ЭВМ в наши дни [4]. Только за один 1988 г. в этой стране ущерб от подобных преступлений оценивался в 550 млн. долл. Потеря-

Таблица 1

США, 1986-1988 гг.

Год	Характер преступления	Подделка документов и данных,%	Денежные преступления	Преступления, связанные с ПО,%	Прочие %
1986		10	45	44	1
1988		34	36	22	8

Таблица 2

Количество организаций (в %), использующих: а) антивирусные программы; в) магнитные карточки

1,45	85 г.	53,14	91 г. (прогноз)	а.
4,8	85 г.	35.7	91 г. (прогноз)	и.

но почти 930 человеко-лет и 15,3 лет чистого машинного времени. В среднем организация, имеющая компьютеры, несет ущерб в 109 тыс.долл., теряет 365 человеко-часов и 26 ч машинного времени на борьбу с нарушителями. Больше других от электронных мошенников страдают коммерческие организации: на их долю приходится 36% всех компьютерных преступлений. Структура электронных преступлений в США за 1986-1988 гг. характеризуется значительным динамизмом (табл.1). В 1988-1989 гг. увеличивается количество преступлений, непосредственно не связанных с денежным обращением. Отчет показывает, насколько интенсивно совершенствовались средства обеспечения компьютерной безопасности начиная с 1985 г. (табл.2).

Все большее распространение получают специальные программы шифрования данных: идентификационные карточки, антивирусные программы. Частные фирмы и государственные учреждения вынуждены приобретать все более совершенные и, следовательно, более дорогие аппаратные и программные средства защиты информации, затраты на эти цели за два последних года выросли на 66%, а доходы от их продажи в 1988 г. составили 588 млн.долл. Предполагается, что к 1993 г. эта цифра достигнет одного миллиарда долларов.

Слабые места вычислительных систем

Вычислительная система (ВС) содержит пять основных компонент, особенно привлекательных для злоумышленников.

Одна из этих компонент — ввод данных. С этой целью используется различное оборудование: считыватели перфокарт и перфоленты, удаленные терминалы, накопители на гибких магнитных дисках, винчестеры и т.д. Очень часто преступление начинается с сознательного искажения вводимых данных или изъятия важных входных документов. Можно заставить ВС оплачивать несостоявшиеся услуги, переводить платежи за закупки, которых в действительности никогда не было, формировать ложный курс акций на бирже, указывать несуществующих пользователей системы массового обслуживания (например, телефонной станции).

Таким образом, в 1988 г. было совершено одно из наиболее значительных компьютерных преступлений — на сумму почти 70 млн.долл. В преступную группу входили семь человек, в том числе двое служащих американского Первого национального банка, один из которых имел непосредственное отношение к процедурам защиты информации. Успешно обойдя систему защиты и подделав

входные данные компьютерной системы оплаты сделок, "электронные грабители" перевели 69,7 млн.долл. на свои счета в Австрийский банк. Преступление было пресечено до того, как средства пошли в оборот, в противном случае пострадавшие фирмы United Airlines, Merrill Lynch & Co, Brown Forman понесли бы значительные убытки. Аналогичный случай имел место и в Англии, где один подросток похитил 985 тыс.ф.ст. из Национального вестминстерского банка. Общественность была поражена той легкостью, с которой вчерашний мальчишка стал миллионером. Кстати, преступление вскрылось только из-за того, что юноша уж очень резко изменил свой образ жизни [4].

Вторая компонента ВС — прикладное и системное программное обеспечение (ПО). Не следует забывать, что компьютер лишь шаг за шагом выполняет инструкции, заложенные человеком в его память. Если программа содержит ошибки или измененные коды — это неизбежно скажется на функционировании всей ВС. Чем сложнее программа, тем более она уязвима для сознательного внесения ошибок и искажений. Разновидностью таких программ является так называемый "троянский конь". Подобная программа, помимо действий, предусмотренных спецификацией, совершает и несанкционированные операции: считывание или запись чужого секретного файла, изменение защищенного участка оперативной памяти ЭВМ, выдачу блокирующих сигналов на внешние устройства, передачу ложных сообщений на другие ЭВМ в составе сети. "Троянский конь" часто тщательно маскируется под обычную программу, стремясь уничтожить все следы несанкционированных действий. Именно так действовали молодые компьютерные взломщики из Западной Германии, успешно проникшие в совершенно секретную базу данных Северо-американского космического агенства (НАСА), имеющую филиалы в ФРГ, Великобритании, Франции, Швейцарии и Японии. Следователи из Западногерманского министерства внутренних дел установили, что компьютерные взломщики ввели в международную компьютерную систему "троянского коня" с универсальным ключевым словом, позволявшим получать сверхсекретную информацию по разработке, применению и производству космического оружия. Молодые люди работали над планом своего "электронного путешествия" более полугода, тщательно анализируя системы защиты и контроля международной сети "СиЭн". Деятельность "взломщиков" пресек служащий, отвечающий за вопросы безопасности одной западногерманской исследовательской лаборатории [16].

ПО может быть не только средством компьютерного преступления, но и его целью. Похищенное ПО может быть продано конкурирующей фирме, размножено с целью коммерческого распространения, наконец, за него может быть потребован выкуп. Утрата ценного ПО выбивает из колеи фирму или организацию вплоть до момента введения в действие дублирующих программ.

Следующий "слабый" элемент ВС — центральный процессор (ЦП). Под его руководством осуществляется выбор данных и команд из ОП ЭВМ. Имеют место многочисленные случаи, когда преступник подключается именно к центральному процессору, ведь он является "мозгом" и "нервной системой" ВС. Особую угрозу представляют попытки вывести из строя ЦП в вычислительных системах, непосредственно связанных с жизнедеятельностью людей, — в медицинских, военных, транспортных и других АСУ.

Четвертый элемент работы ВС — выдача результатов. Выходные данные могут быть изменены или похищены в корыстных целях. В качестве примера можно привести случай, когда почтовый реестр крупной издательской фирмы был продан группой служащих конкурирующему издательству.

Более подробно остановимся на

пятом, весьма важном аспекте работы системы — процессе связи. При эксплуатации ВС данные передаются между ЭВМ и терминалом или от одной машины к другой в обоих направлениях. Этот процесс доступен для постороннего вмешательства и представляет собой весьма слабое место с точки зрения безопасности ВС. Наиболее часто используемые видами подобных атак на ВС, получивших название "электронное проникновение", являются ответвление линий связи и электромагнитный перехват.

В первом случае к линии связи или непосредственно к ЭВМ подключается устройство, предназначенное для перехвата и записи сообщений. Пользуясь таким устройством, преступник может не только получить доступ к секретной информации, но и подделывать чужие сообщения, влияя таким образом на процесс принятия решений в ВС.

Электромагнитный перехват основан на использовании специальных технических средств, способных регистрировать электромагнитные поля, создаваемые различными узлами ЭВМ и периферийными устройствами. Такие приспособления способны действовать на значительном расстоянии от объектов ВС. Широкое распространение получил метод проникновения в ВС, называемый вхождением между строк. В этом случае к линии связи подключается дополнительный терминал, и работающий на нем человек устанавливает связь с системой в тот момент, когда какой-либо легальный ее пользователь не работает с системой, но держит канал связи занятым. При недостаточном внимании администрации ВС к проблемам безопасности информации "вхождение между строк" обнаруживается очень трудно.

Так, в штате Нью-Джерси (США) преступник воспользовался вышеуказанным способом проникновения в ВС для внедрения в компьютеры своего бывшего шефа вируса типа "бомба замедленного действия". Хотя ущерб превысил 75 тыс. долл., он мог бы быть и большим, если бы пострадавшая компания не имела на вооружении специальные программы обеспечения безопасности. Они позволили провести трассировку и "вычислить" нарушителя, которому по законам штата грозит до 10 лет тюрьмы и 100 тыс. долл. штрафа [5].

Приведенные выше примеры показывают, насколько уязвимы незащищенные вычислительные системы. Информация, циркулирующая в них, может быть незаконно изменена, похищена, уничтожена. Последствия же подобных действий в наш электронный век — самые серьезные.

К счастью, существует ряд способов и мер, позволяющих значительно снизить угрозу компьютерных преступлений, — ведь против любого яда рано или поздно находится противоядие.

Криптология — наука о защите информации

Проблемы защиты информации волновали человечество с незапамятных времен. Как надежно передать секретные военные сведения? Является ли тот или иной документ подлинным? Можно ли тайно сообщить важные политические новости главе государства? От ответов на эти вопросы зависели судьбы целых народов.

Первые системы шифров мы встречаем в Древнем Египте и Древней Греции, Риме и Спарте. Заботилась о секретности информации правящая верхушка в Венеции (Совет десяти) в XYI в. Без знания специального ключа бесполезно читать труды многих ученых средневековья — одни боялись преследования инквизиции, другие заботились о пальме первенства, третьи хотели, чтобы их знания достались только узкому кругу избранных учеников. Примеры достаточно сложных зашифрованных текстов встречают археологи и в русских памятниках XII-XIII вв. Так что наука, получившая название "криптология" (от греческих корней: CRYPTOS — тайный и LOGOS — слово), имеет древние

корни и традиции. Она довольно четко может быть разделена на два направления: криптографию и криптоанализ.

Задача криптографа — обеспечить как можно большую секретность и аутентичность (подлинность) передаваемой информации. Криптоаналитик, напротив, "взламывает" систему защиты, разработанную криптографом. Он пытается раскрыть зашифрованный текст или выдать поддельное сообщение за настоящее.

Одним из основных допущений криптографии является то, что криптоаналитик имеет полный шифротекст и ему известен алгоритм шифрования, за исключением секретного ключа. При этом предполагается, что криптоаналитику доступен для анализа только шифротекст.

На практике, однако, приходится сталкиваться и с другими ситуациями. Так, для криптоанализа может стать доступен не только шифрованный текст, но и часть соответствующего открытого текста. В этом случае криптограф должен разрабатывать систему, стойкую к анализу на основе открытого текста. В случае, если криптограф допускает, что противник способен "прогнать" через систему свой собственный открытый текст и получить соответствующий шифротекст, он должен разрабатывать систему, стойкую к анализу на основе выбранного открытого текста. Можно представить и следующую ситуацию: криптоаналитик навязывает свой собственный шифротекст и наблюдает текст, в который он преобразует в процессе дешифрации. В этом случае говорят о стойкости шифросистемы к анализу на основе выбранного шифротекста. Наконец, различные из перечисленных выше ситуаций могут комбинироваться.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Поэтому за рубежом различное криптографическое оборудование находит весьма широкое применение: от закрытия информации в специальных компьютерных сетях до серийно выпускаемых защищенных телефонных аппаратов.

Зарубежными специалистами сформулирована следующая система требований к алгоритму шифрования, предназначенному для массового применения в ВС [16]:

1) зашифрованный текст должен поддаваться чтению только при наличии ключа шифрования;

2) число операций, необходимых для определения использованного ключа шифрования по фрагменту шифрованного текста и соответствующего ему открытого текста, должно быть не меньше общего числа возможных ключей;

3) знание алгоритма шифрования не должно влиять на надежность защиты;

4) незначительные изменения ключа шифрования должны приводить к существенному изменению вида зашифрованного текста;

5) незначительные изменения шифруемого текста должны приводить к существенному изменению вида зашифрованного текста даже при использовании одного и того же ключа;

6) структурные элементы алгоритма шифрования должны быть неизменными;

7) в процессе шифрования дол-

жен осуществляться постоянный контроль за шифруемыми данными и ключом шифрования;

8) дополнительные биты, вводимые в текст в процессе шифрования, должны быть полностью и надежно скрыты в шифрованном тексте;

9) длина шифрованного текста должна быть равной длине исходного открытого текста;

10) не должно быть простых и легко устанавливаемых зависимостей между ключами, последовательно используемыми в процессе шифрования;

11) любой ключ из множества возможных должен обеспечивать надежную защиту информации;

12) алгоритм должен допускать как программную, так и аппаратную реализацию, при этом изменение длины ключа не должно вести к качественному ухудшению алгоритма шифрации.

В настоящее время два общепринятых алгоритма шифрации могут претендовать на то, чтобы в достаточной мере удовлетворять перечисленным требованиям. Речь о них пойдет ниже.

DES — стандарт шифрования данных

В 1972 г. Национальное бюро стандартов (NBS), подчиняющееся Министерству торговли США, выдвинуло программу разработки стандартов по защите данных ЭВМ от несанкционированного доступа. Стандарты требовались в таких областях, как шифрование, установление подлинности личности и данных (аутентификация), контроль доступа, надежное хранение и передача данных.

В результате плодотворного сотрудничества трех организаций-Национального бюро стандартов, Управления национальной безопасности (NSA) и фирмы IBM подобный стандарт, получивший название DTS (Data Encryption Standart) был разработан и опубликован 17 марта 1975 г. в специальном издании Federal Register.

Алгоритм DES был разработан в виде стандарта функциональной совместимости, предусматривающего полную спецификацию основной функции и формата и в то же время независимость от физической реализации. Его публикация вызвала оживленную полемику среди специалистов в области защиты информации. Последовал ряд практических замечаний и попыток дискредитации принятого алгоритма. Поскольку NBS начало разработку DES, оно отвечало за соответствие предлагаемого стандарта всем требованиям и за его приемлемость для многих потенциальных пользователей. После двухлетних исследований организации, возглавлявшие работу по созданию стандарта (NBS, NSA и IBM), решили, что окончательный вывод должен быть сделан в ходе публичного обсуждения стандарта DES. NBS организовало два симпозиума: один по математическим аспектам алгоритма с целью поиска в нем "тайной лазейки", а другой — по экономическим вопросам, в частности, по установлению длины ключа.

Сразу же после прохождения симпозиумов было принято решение оставить стандарт без изменений. В алгоритме не было установлено никаких "лазеек". Эффективная длина ключа в 56 бит вполне удовлетворяла потенциальных пользователей на ближайшие 10-15 лет, так как общее количество ключей в этом случае оценивалось цифрой $7{,}6 \times 10^{16}$.

Необходимо подчеркнуть, что стандарт DES стал одним из первых "открытых" шифроалгоритмов. Все схемы, используемые для его реализации, были опубликованы и тщательно проверены. Секретным был только ключ, с помощью которого осуществляется кодирование и декодирование информации.

Алгоритм DES базируется на блестящей работе Шеннона 1949 г., связавшей криптографию с теорией информации [8]. Шеннон выделил два общих принципа, используемых в практических шифрах: рассеивание и перемешивание. Рассеиванием он назвал распространение влияния одного

знака открытого текста на множество знаков шифротекста, что позволяет скрыть статистические свойства открытого текста. Под перемешиванием Шеннон понимал использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифрованного текста. Однако шифр должен не только затруднять раскрытие, но и обеспечивать легкость шифрования и дешифрования при известном секретном ключе. Поэтому возникла идея использовать произведение простых шифров, каждый из которых вносит небольшой вклад в значительное суммарное рассеивание и перемешивание.

В составных шифрах в качестве элементарных составляющих чаще всего используются простые подстановки и перестановки.

Подстановка относится к простейшим методам шифрования. Ключом является переставленный алфавит, буквами которого заменяют буквы нормального алфавита. Так, если букву А заменить на Б, Б на В и т.д., то слово ЗАЩИТА будет выглядеть как ИБЭКУБ. Шифрование простой подстановкой на коротких алфавитах типа латинского и русского обеспечивает слабую защиту лежащего в основе открытого текста. Дело в том, что распределение частот отдельных символов в открытом тексте сохраняется неизменным и в шифротексте.

Однако, если подстановка делается в очень большом алфавите, а вероятность повторения каждого символа открытого текста в течение времени использования одного ключа мала, то статистические свойства шифра дают очень мало информации криптоаналитику, и шифр становится достаточно стойким.

В случае перестановки переставляются не буквы алфавита, а буквы в сообщении открытого текста. Распределение частот отдельных символов оказывается в шифрованном тексте то же, что и в открытом тексте, однако распределения более высоких порядков оказываются перемешанными. В качестве примера рассмотрим перестановку, задаваемую таблицей

1 2 3 4 5 6
6 4 2 1 3 5

При этом открытый текст разбивается на отдельные сообщения по 6 символов, и в каждом сообщении буквы переставляются в соответствии со следующим правилом: первый знак становится шестым, второй — четвертым и т.д. Тогда слово "защита" преобразуется в "ищтффз". Если к результату перестановки применить описанную выше подстановку, получим Кэубби. При многократном чередовании простых перестановок и подстановок можно получить очень стойкий шифр (криптоалгоритм) с хорошим рассеиванием и перемешиванием.

Стандарт шифрования данных (DES) — один из наиболее удачных примеров криптоалгоритма, разработанного в соответствии с принципами рассеивания и перемешивания. В нем открытый текст, криптограмма и ключ являются двоичными последовательями длиной соответственно $M = 64$, $N = 64$ и $K = 56$ бит. Криптоалгоритм DES представляет собой суперпозицию элементарных шифров, состоящую из 16 последовательных шифроциклов, в каждом из которых довольно простые перестановки сочетаются с подстановками в 4-битовых группах. В каждом проходе используются лишь 48 бит ключа, однако они выбираются внешне случайным образом из полного 56-битового ключа.

DES-алгоритм используется как для шифрования, так и для установления подлинности (аутентификации) данных. Он способен функционировать в четырех основных режимах: электронной кодовой книги (ECB), обратной связи по шифротексту (CFB), сцепления блоков шифра (CBC) и обратной связи по выходу (OFB) [7]. Каждому режиму свойственны свои преимущества и недостатки. Режим ECB очень хорошо подходит для шифрования ключей; режим CFB обычно предназначается для шифрования отдельных символов, режим

OFB нередко применяется для шифрования в спутниковых системах связи.

Режимы CBC и CFB пригодны для аутентификации данных. Они позволяют использовать алгоритм DES при обмене данными между терминалом и главной ЭВМ, шифровании криптографического ключа в процедурах автоматизированного распределения ключей, шифровании файлов, почтовых отправлений, спутниковой информации и для ряда других практических задач.

Прошло уже больше 15 лет с момента опубликования DES в открытой литературе. Несмотря на интенсивные и тщательные исследования алгоритма специалистами, сообщений об его уязвимых местах не поступало. Единственное средство для его "взлома" — полный перебор ключей. Как уже упоминалось, это сделать весьма непросто: для проведения подобной силовой атаки, последовательно использующей каждый из $2^{56} \approx 10^{17}$ ключей, требуется построение специализированной многопроцессорной ЭВМ стоимостью около 20 млн.долл.[7].

Криптографические системы с открытым ключом

Криптография с открытым ключом окончательно оформилась как самостоятельное направление в теории защиты информации в мае 1975 г. Появлению нового направления способствовали две проблемы, которые не могли быть разрешены в рамках классических криптографических схем.

Первая из этих проблем связана с распространением секретных ключей. В больших коммерческих сетях число возможных соединений между пользователями определяется формулой $(n^2-n)/2$, где n — число пользователей [6]. В системе с одним миллионом пользователей возможно около $5 \cdot 10^{11}$ соединений, и стоимость распространения ключей оказывается неприемлемо высокой.

Вторая — это проблема электронной подписи. В конце письма или другого авторизованного документа исполнитель обычно ставит свою подпись. Подобное действие преследует две цели: во-первых, получатель имеет возможность убедиться в истинности письма, сличив подпись с имеющимся у него образцом; а во-вторых, личная подпись является юридическим гарантом авторства документа. Последний аспект особенно важен при заключении разного рода торговых сделок, составлении доверенностей, обязательств и т.д.

Обе проблемы казались трудноразрешимыми. Действительно, наличие секретного ключа, известного только получателю сообщения и его отправителю, столетиями считалось непременным условием безопасной передачи информации.

Однако подделать подпись человека на бумаге весьма непросто, а скопировать цепочку битов на ЭВМ — пустяковая операция. Кто сможет в этом случае гарантировать подлинность и авторство сообщений?

Обе проблемы были успешно решены единым методом — криптографией с открытыми ключами. В основе этого метода лежат так называемые односторонние, или необратимые, функции: при заданном значении x относительно просто вычислить значение f(x), однако, зная y = f(x), определить x чрезвычайно трудно.

Приведем также строгое определение криптографической системы с открытым ключом — СОК [6]. Подобная система представляет собой пару семейств алгоритмов $\{E_к\}$, $к \in \{K\}$ и $\{D_к\}$, $к \in \{K\}$, определяющих обратимые преобразования:

$E_к$: $\{M\} \to \{M\}$

$D_к$: $\{M\} \to \{M\}$

на конечном пространстве сообщений {M}, таких, что:

1) для каждого $к \in \{K\}$, $D_к$ обратно к $E_к$, т.е. при любых к и M $D_к \cdot E_к(M) = M$;

2) для каждого $к \in \{K\}$ и $m \in \{M\}$ нетрудно вычислить $E_к(M)$ и $D_к(M)$;

3) для почти каждого $к \in \{K\}$ невозможно в вычислительном отноше-

нии вывести из $E_к$ какой-либо легко вычислимый алгоритм, эквивалентный $D_к$;

4) по каждому к $\in$ {K} можно получить инверсную пару $E_к$ и $D_к$.

Причина, по которой ключи в обычных криптографических системах должны столь тщательно защищаться, состоит в том, что функции шифрования и дешифрования в ней неразделимы. Любое лицо, получившее ключ для шифрования, может также дешифровать сообщения.

Описанное выше третье свойство систем с открытыми ключами позволяет не засекречивать ключи шифрования пользователя $E_к$ без ущерба для секретности его ключа дешифрования $D_к$ (и наоборот, можно оставить в секрете лишь ключ дешифрования $D_к$, а ключ шифрования $E_к$ не защищать).

Четвертое свойство гарантирует реализуемость системы с открытыми ключами на практике. Обычно криптографическое оборудование подобных систем содержит генератор псевдослучайных чисел, образующий значение параметра К, и аппаратуру, реализующую соответствующие функции $E_к$ и $D_к$.

Посмотрим теперь, как с помощью СОК можно решить проблему распределения ключей в системе с множеством пользователей.

Каждый пользователь генерирует пару взаимно обратных преобразований E и D. Преобразование D он держит в секрете (личный ключ), а преобразование E (открытый ключ) публикуется в открытом справочнике наподобие телефонного.

Каждый, кто хочет установить связь с данным пользователем, находит его имя в справочнике, выполняет над сообщением соответствующее преобразование E и посылает его по линии связи. Расшифровать сообщение может только законный получатель, обладающий секретным ключом дешифрации D.

СОК решают и проблему электронной подписи. В этом случае пользователь A, желающий послать подписанное сообщение M пользователю B, шифрует его с помощью своего личного ключа D_a, получая "подписанное" сообщение $S = D_a(M)$. Получив сообщение S, пользователь B получает M с помощью открытого ключа E_a, предварительно помещаемого пользователем A в справочник.

Пользователь B сохраняет сообщение S как доказательство того, что пользователь A действительно прислал ему данное сообщение M. Если позднее A откажется от факта посылки этого сообщения, то B может предъявить суду сообщение S. Так как Ea находится в открытом файле, суд имеет возможность получить сообщение $M = E_a(S)$, которое содержит имя A, дату, время и т.д. Сообщение S мог послать только A, так как только он знает секретный ключ D_a.

Этот метод обеспечивает надежное установление авторства или подлинности электронных документов, но не секретность связи.

Действительно, любой желающий может взять открытый ключ E_a из справочника и получить M. Так что, если требуется секретность передаваемого сообщения, A должен воспользоваться открытым ключом $E_в$ и послать вместо S сообщение $S' = E_в(S)$. Пользователь B дешифрирует S' с помощью личного ключа $D_в$ и восстанавливает S. После этого, применяя открытый ключ E_a, он получает сообщение M. Действия, предпринимаемые для доказательства авторства сообщения, остаются без изменений.

Несмотря на довольно большое число различных СОК, практическое воплощение получила только одна — RSA, получившая название в честь ее изобретателей — Ривеста, Шамира и Эйдлмэна. (R.Rivest, A.Shamir, L.Adlman).

Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, но разложение на множители произведения двух таких чисел практически невыполнимо. Пользователь случайным образом выбирает два достаточно больших (например, 100-битных) числа P и

Q и перемножает их, получая число N. Число N опубликовывается, но множители P и O содержатся в секрете. Используя их, можно вычислить специальную функцию Эйлера Ф(N) (количество целых чисел, меньших N и взаимно простых по отношению к N) как Ф(N) = (P-I)(Q-I). Затем случайным образом выбирается число из интервала от 2 до Ф(N). Это число, назовем его E, также публикуется. Таким образом, открытый ключ шифрования представляет собой пару целых чисел (N, E).

Зашифрование исходного блока текста M производится следующим образом: $C = M^E (\mathrm{mod}\ N)$, $0 < M < N$, C — шифрованный текст. В качестве дешифрующего секретного ключа используется число D, такое, что $ED = 1 \bmod Ф(N)$. Такое число легко вычисляется, если известны секретные числа P и Q. Дешифрация осуществляется возведением C в степень D по модулю N, $M = C^D (\mathrm{mod}\ N)$, $0 < C < N$.

Задача определения при известных числах N и E ключа D в общем случае эквивалентна трудоемкой задаче отыскания разложения числа на простые множители P и Q, хотя известны примеры таких пар (N, E), для которых решение этой задачи выглядит гораздо проще [9].

Система RSA получила достаточно широкое распространение как в США, так и в других странах. Появление первой серийной интегральной схемы, реализующей метод RSA, состоялось в результате успешной работы корпорации Cylink в середине 80-х годов [10].

Выпускаемое в настоящее время серийное устройство CY 1024 осуществляет преобразование над модулями размером более 16 тыс.бит. Скорость работы устройства, достигающая 1000 бит в секунду, а также его размеры удовлетворяют предъявляемым требованиям для многих приложений.

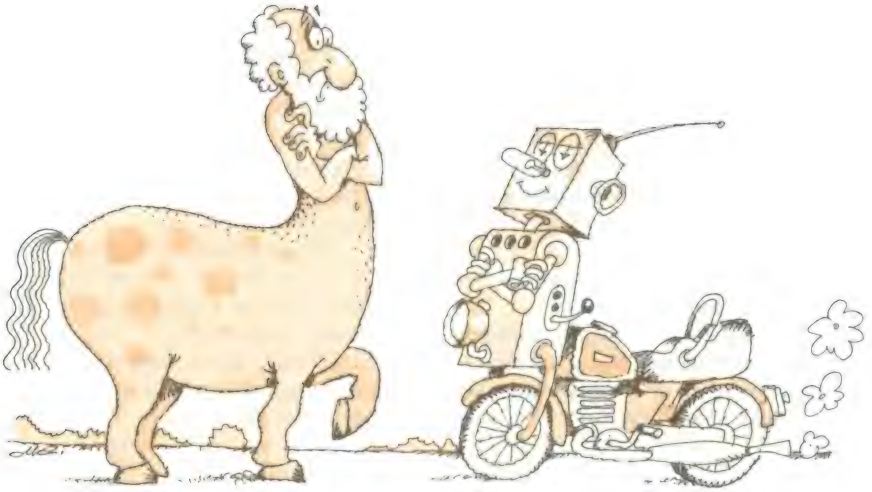
Как повысить защищенность вашей ВС

Ряд достаточно простых, но эффективных мероприятий поможет существенно улучшить защищенность вашей ВС. Специалисты по компьютерной безопасности рекомендуют:

1) Производить четкое распределение обязанностей между сотрудниками, связанными с обработкой информации в ВС.

Необходимо выделить прикладных и системных программистов, администраторов системы, пользователей из внешних организаций. Желательно, чтобы эти группы не пересекались.

2) Ограничивать допуск к ЭВМ, хранилищам дисков и лент, докумен-



тации и другим важным печатным формам (чеки, бланки и т.д.).

Многие установки по обработке данных охраняются очень небрежно — к ним имеет доступ буквально каждый. Контроль обычно ослабевает к концу недели, месяца, квартала. Не случайно подавляющее большинство компьютерных преступлений совершается именно в эти дни.

3) Внедрять системы встроенного контроля.

Там, где речь идет об особо важных вопросах, следует организовать внешний контроль силами той части организации, которая не связана с процедурами обработки данных. Все терминалы должны работать под программным контролем, процедуры вхождения в систему периодически распечатываться и анализироваться.

4) Тщательно контролировать изменения, вносимые в системные файлы и программы.

5) Вводить в штат администрации ВС специалиста в области компьютерной безопасности.

6) уделять значительное внимание вопросам аутентификации объектов и субъектов ВС (ниже речь об этой проблеме пойдет подробно).

7) Подходить к известным случаям нарушения безопасности ВС следующим образом: "Это может случиться и в нашей организации, но это не должно произойти".

Одно из наиболее узких мест в проблеме безопасности ВС — установление подлинности объектов вычислительной среды: пользователей, сообщений и удаленных станций (терминалов, ПК или больших ЭВМ). В специальной литературе установление подлинности часто обозначается термином "аутентификация", от английского authentication.

В проблеме аутентификации можно выделить три аспекта.

1) Задача аутентификации пользователя — является ли пользователь, обращающийся к тем или иным ресурсам ВС, тем, за кого он себя выдает?

2) Задача аутентификаии вызываемой станции — является ли станция, ответившая на запрос пользователя, именно той, которую он вызвал?

3) Задача аутентификации сообщения — соответствует ли сообщение, переданное по каналам связи, своему начальному виду?

Остановимся более подробно на первом из указанных аспектов, так как проблема идентификации пользователя возникает в любой ВС, к которой предъявляются хотя бы минимальные требования по безопасности.

Кроме того, ряд мер, предлагаемых ниже, администрация ВС может внедрить буквально на следующий день после ознакомления с ними, что существенно повысит защищенность ВС.

Стандартный подход к обеспечению надежной аутентификации пользователей ВС состоит в постановке одного за другим ряда защитных "барьеров" таким образом, что нарушитель, преодолев один барьер, тут же сталкивается со следующим и т.д. Хотя отдельные барьеры могут быть преодолены легче, чем другие, в целом система защиты оказывается достаточно надежной.

Специалисты в области безопасности ВС обычно рекомендуют.

1) Защищать помещение, где находятся терминалы ВС (применяются специальные магнитные карточки, кодовые замки, дежурство лиц, отвечающих за безопасность).

2) Ограничивать число пользователей, которые могут включать терминалы (например, каждый терминал включается только с помощью специального ключа).

3) Контролировать работу пользователей с активных терминалов с помощью паролей.

4) Осуществлять управление процессами доступа к различным базам данных (чаще всего используется парольная защита).

5) Шифровать конфиденциальную информацию с помощью достаточно стойкого алгоритма.

Как мы видим, четыре из пяти основных рекомендаций имеют самое

непосредственное отношение к аутентификации пользователя, иными словами, к установлению того, действительно ли данный пользователь является тем, за кого он себя выдает. Существуют два основных подхода к установлению подлинности пользователя. Первый основан на сравнении с хранящимся эталоном некоторых "природных" характеристик испытуемого: голоса, отпечатков пальцев, почерка, геометрии руки и т.д. Достаточно полный обзор подобных методов аутентификации приведен в [11]. Всем им, к сожалению, присущи два недостатка.

Первый. Компьютерная программа или специальное устройство анализирует совершенно конкретные параметры человека (обычно не более 12-16), представленные в ЭВМ в виде дискретных отсчетов функции, которая в реальности непрерывна. Если нарушитель уложится в этот "зазор", то система защиты опознает его как владельца хранящихся характеристик.

Второй. Характеристики, хранящиеся в ЭВМ, могут быть подделаны. Эта общая опасность для многих систем ограничения доступа, основанных на проверке того или иного характерного свойства, — хранящиеся эталоны должны быть очень хорошо защищены!

Второй подход к установлению подлинности пользователя базируется на наличии у последнего некоторых "искусственных" физических объектов (специальные ключи, магнитные карточки и т.д.), либо на сугубо личной и хранимой в тайне от других лиц информации (пароль, девичья фамилия жены, день рождения бабушки и т.д.).

Отметим недостатки этого подхода. Физические объекты, используемые для аутентификации, трудно при необходимости изменить, они часто теряются (или выкрадываются), а также подвержены угрозам копирования или имитации.

Парольная защита распространена очень широко, она внедрена во многих организациях нашей страны. Однако часто при этом не достигается достаточного эффекта. Ниже приводятся основные причины такого состояния.

1) Администрация ВС задает слишком длинные пароли. Будучи не в состоянии их запомнить, пользователи записывают пароли на клочках бумаги, в записные книжки и т.д. После этого пароль теряет все свои привлекательные черты и становится физическим объектом, который очень легко подделать.

2) Пользователи склонны к выбору тривиальных паролей (например, год рождения, фамилия), которые элементарно "взламываются" после нескольких попыток.

3) Процесс ввода пароля в систему поддается наблюдению даже в том случае, если отсутствует режим "эхо", — вводимые символы не отражаются на экране терминала. Вы можете поставить эксперимент и убедиться, с какой высокой скоростью необходимо набирать на клавиатуре пароль, чтобы находящийся рядом человек не мог бы зафиксировать его в памяти. Вводя пароль, убедитесь, что никто не стоит за вашей спиной.

4) Существует таблица паролей, обычно входящая в состав ПО операционной системы. При недостаточном внимании к ее защите таблица может быть изменена, что зачастую и происходит. Кодируйте таблицу паролей! Ключ алгоритма декодирования должен находиться только у администратора ВС или лица, отвечающего за безопасность информации.

5) Известны случаи, когда в ВС вносится "троянский конь", перехватывающий вводимые пароли и записывающий их в отдельный файл. Применяйте усовершенствованные способы парольной защиты, которые будут описаны ниже, с целью избежать подобной угрозы.

Как оценить стойкость парольной защиты

По своей сути, пароль представляет собой последовательность букв некоторого алфавита и специальных

знаков, удовлетворяющую ограничению на наибольшую и наименьшую длину. Какие конкретные значения необходимо задавать для мощности множества букв и специальных символов? Какова должна быть оптимальная длина пароля?

От правильных ответов на этот вопрос зависит безопасность вашей ВС. Вопросы устойчивости паролей впервые были популярно изложены в классической работе по защите информации Хоффмана [12]. Здесь мы хотели бы показать взаимосвязь между различными параметрами, входящими в так называемую формулу безопасности, позволяющую рассчитывать среднее время надежного существования парольной системы защиты [13].

Зададим следующие обозначения:

R — скорость ввода информации в ВС (симв/ед.врем.);

C — число символов, вводимых в компьютер в течение процедуры допуска;

L — число символов в пароле (т.е.длина пароля);

S — мощность множества, из которого извлекаются символы для пароля;

P — вероятность успешного "взлома" системы защиты;

$T_б$ — среднее время безопасности (математическое ожидание случайной величины, характеризующей интервал времени, в течение которого система защиты не поддается взлому);

T — время, в течение которого нарушитель предпринимает систематические попытки "взломать" систему защиты;

d — временная задержка (интервал времени между двумя неудачными попытками войти в ВС). Специально вводится администрацией ВС с целью уменьшить количество попыток "взломать" систему защиты за некоторый интервал времени; $d = 1$ — если задержки нет, $d > 1$ — в противном случае.

Среднее время безопасности задается выражением (формула безопасности): $T_б = (d \cdot C/R) \cdot S^L/2$, где значение $d \cdot C/R$ определяет полное время, затрачиваемое нарушителем на одну попытку подбора пароля; S^L — общее количество возможных паролей.

Пусть N_2 — количество попыток подбора пароля за время T. Тогда $N_2 = T/(d \cdot C/R) = (T \cdot R)/(d \cdot C)$.

Нижняя грань, P_o, для вероятности P: $P_o = N_2/S^L = (T \cdot R)/(d \cdot C \cdot S^L)$.

Наконец, поскольку $P \leqslant P_o$, мы можем оценить вероятность взлома системы защиты: $P \geqslant (T \cdot R)/(d \cdot C \cdot S^L)$.

Теперь администрация ВС обладает простым и эффективным средством для определения тех или иных конкретных параметров, входящих в формулу безопасности.

Предположим, необходимо вычислить необходимую длину пароля при прочих фиксированных параметрах. Так как $S^L = (T \cdot R)/(P_o \cdot d \cdot C)$, можем записать $L = [\log(T \cdot R) - \log(P_o \cdot d \cdot C)]/ \log(S)$. Практически полезным может оказаться и выражение $T = P \cdot S^L \cdot d \cdot (C/R)$, показывающее связь между временем, которым располагает потенциальный "взломщик", и другими параметрами системы защиты.

Несколько слов необходимо сказать о том, почему возникла необходимость вводить понятия "нижняя грань" (P_o) для вероятности проникновения нарушителя в ВС за время T. Дело в том, что злоумышленник после каждой неудачной попытки "взома" вычеркивает из списка возможных паролей одно значение. Таким образом, если, например, система защиты содержит максимум 1000 паролей, то за 999 попыток преступник с вероятностью 1 подберет необходимое значение. Другое дело, если система организована таким образом, что после каждой неудачной попытки входа в ВС она автоматически переходит на некоторое новое значение пароля. Естественно, процесс перехода должен быть согласован с законным пользователем — обладателем начального пароля. В этом случае взломщик оказывается в гораздо более тяжелых условиях: нельзя вычеркнуть испробованный пароль из

списка возможных, ведь система защиты может перейти на него через несколько шагов.

Существуют различные способы согласования перехода на новое значение пароля, наиболее оптимально применение устройства, обеспечивающего переход в заданном пространстве паролей по псевдослучайному закону с равномерным законом распределения. Как показали авторы данной статьи, в этом случае среднее время безопасности системы защиты увеличивается в 2 раза. Следует применять такую схему или нет, необходимо решать в каждом конкретном случае, так как она значительно повышает стоимость аппаратуры и создает определенные сложности для пользователей, которые случайно ошиблись при наборе пароля.

Защита паролей

Существуют различные способы защиты паролей. Наиболее простой заключается в шифровании таблицы паролей, хранящейся в памяти ЭВМ. В этом случае пользователь вводит свой пароль в открытом виде, а компьютерная программа (или специальная микросхема) кодирует его и сравнивает с хранящимся эталоном. Тем самым достигается защита от считывания и копирования таблицы паролей, однако все сказанное выше относительно возможности похищения паролей, заданных в открытом виде, остается в силе. В частности, в ВС может быть внесен "троянский конь", перехватывающий вводимый пользователем пароль еще до этапа шифрования.

Второй метод рекомендует использовать "одноразовые" пароли. Пользователь обладает списком паролей, каждый из которых применяется только один раз, после чего уничтожается в памяти ЭВМ и вычеркивается из списка у пользователя. При этом перехват пароля становится бессмысленным — его значение не повторяется.

Метод не свободен от недостатков. Во-первых, необходимо где-то хранить список паролей, запомнить его практически невозможно. Во-вторых, возникают чисто административные трудности: список может занимать достаточно большой объем памяти в ЭВМ, его необходимо постоянно изменять и т.д.

Третий метод кодирования паролей основан на идее "персонального физического ключа". В памяти компьютера хранится таблица, в которой записаны как пароли в зашифрованном виде, так и их открытый вариант. Кроме того, лицам, допущенным к работе в ВС, выдается специальная магнитная карточка, на которую занесена информация, управляющая процессом шифрования. Заметим, что этой информации внутри компьютера не существует. Процедура допуска требует, чтобы пользователь вставил карточку в специальное считывающее устройство и ввел свой пароль в открытом виде. После этого пароль кодируется с использованием информации, записанной на магнитной карточке, и ищется соответствующая точка входа в таблицу паролей. В случае, если закодированный пароль соответствует хранящемуся эталону, подлинность пользователя считается установленной.

Какие же недостатки у последнего метода? Прежде всего, существует угроза того, что нарушитель, анализируя пары "шифрованный пароль" — "открытый пароль", сможет "расколоть" алгоритм кодирования. Поэтому рекомендуется использовать хорошо зарекомендовавшие себя схемы типа RSA и DES. Помните о том, что "кустарные" алгоритмы легко поддаются криптоанализу! Кроме того, компьютерный взломщик может попытаться применить полученные знания для дешифрования файлов, содержащих секретную информацию. Вот почему необходимо кодировать пароли и файлы с помощью разных схем кодирования, или как минимум применяя различные ключи.

Ряд перспективных идей, связанных с защитой паролей, основан на теории открытых ключей [10]. Поль-

зователь обладает как открытым (публичным) ключом, так и секретным (личным). Зная ключ кодирования, ключ декодирования восстановить очень трудно. Процедура допуска выглядит следующим образом: с помощью личного ключа пользователь образует пароль и передает его в компьютер. Компьютер генерирует некоторое случайное число и сообщает его пользователю. Далее случайное число кодируется с помощью личного ключа пользователя и возвращается в ЭВМ, где происходит его дешифрование и сравнение с оригиналом. Поскольку случайное число никогда не повторяется от сеанса к сеансу (оно может основываться, например, на времени и дате сеанса связи), то перехват этой информации теряет смысл. В памяти ЭВМ хранятся только "открытые" параметры системы кодирования, так что их похищение также бесполезно. Специалисты в области защиты информации считают, что возможности метода открытых ключей для аутентификации еще далеко не исчерпаны [9].

Ниже приводится таблица, позволяющая сравнить различные методы ограничения доступа в ВС по ряду параметров [13]. Условные обозначения имеют следующий смысл (см.табл.3):

,+, — метод имеет преимущества;

,-, — метод обладает недостатками;

,*, — необходимо осуществить выбор: если в конкретной реализации метод будет обладать достоинствами по одному критерию, то по другому — недостатками.

Подобные "взаимообратные" критерии располагаются в соседних столбцах.

Компьютерный вирус

Читатель, видимо, уже знаком с понятием "компьютерный вирус" (КВ). Начиная где-то с 1984 г. этот термин не сходит со страниц массовых изданий, ему посвящаются специальные выпуски серьезных научных исследований, семинары и конференции. Редко кто из опытных программистов в настоящее время не имеет в своей библиотеке программ антивирусных средств. Некоторые из них собрали целые "аптечки" из 10-15 наименований. Подобное коллекционирование не лишено серьезных оснований — электронная эпидемия, захлестнув страны Запада, все шире охватывает и нашу страну.

История КВ связана с именем Фрэда Коэна, известного специалиста

Таблица 3

Ме-\Критетод рий	Не требует запоминания	Препятствует подбору	Прост в обращении	Препятствует перехвату и копированию	Не создает угрозы взлома системы шифрования	Препятствует обману	Способность к немедленной реализации	Относительная стоимость реализации
Шифрование паролей	*	*	+	-	-	-	+	Низкая
Одноразовые пароли	-	-	-	+	-	+	+	Средняя
Магнитные карточки	+	+	+	-	+	-	+	Средняя
Личные ключи	*	*	+	-	+	-	+	Низкая
Открытые ключи с динамическим паролем	+	+	+	+	+	+	-	Высокая

в области компьютерной безопасности, научного сотрудника университета г.Цинциннати (шт.Огайо). Работая над проблемой защиты от несанкционированного копирования ПО, Коэн написал небольшую программу, которая обладала способностью к быстрому самовоспроизведению и совершению различных деструктивных действий: стиранию важной информации на системном диске, уничтожению файлов, изменению системных переменных в ОП ЭВМ и т.д. Программа-вирус активизировалась в случае незаконного копирования исходной авторской программы.

Работа Ф.Коэна привлекла широкое внимание специалистов и была опубликована в материалах национальной конференции по компьютерной безопасности, состоявшейся в 1984 г. Трудно сказать, стала ли публикация толчком к взрывному распространению программ-вирусов, однако начиная именно с этого момента "компьютерная чума XX века" начала свое победное шествие по странам Западной Европы, а затем США, поразив тысячи компьютеров различных фирм, государственных учреждений, научных лабораторий и университетов.

Проблема оказалась гораздо более трудноразрешимой, чем представлялось вначале. КВ способен инфицировать тысячи компьютеров, объединенных в составе информационной сети, буквально за несколько часов. По оценкам экспертов, в США только за один 1988 г. действием компьютерного вируса объяснялось около 50 тыс. случаев нарушения нормального функционирования информационно-вычислительных систем. Компьютерные вирусы поражали ПК в университетах штатов Делавэр, Вайоминг, Пенсильвания, Университетах Дж.Вашингтона и Джорджтауном, в колледжах в Бови (шт.Мэриленд) и Аламеде (шт.Калифорния), а также во многих других высших учебных заведениях США. Имеются сведения об инфицировании компьютеров министерств обороны и юстиции США, ЦРУ, ФБР и НАСА. Среди промышленных фирм наиболее пострадали "Эппл", АТТ, "Арко" и другие корпорации, производящие ПК [14].

Распространяются КВ и в СССР, где главным источником заражения становится незаконное копирование программных продуктов. Отсутствие в нашей стране специальных законодательных актов, регулирующих куплю-продажу ПО, слабая юридическая проработка вопросов авторского права вынуждают производителей программ прибегать к ряду вынужденных мер защиты от несанкционированного копирования, в том числе внесению КВ.

Характерный пример поражения вирусом одного из академических институтов СССР описан в [15]. IBM PC XT, работавшая ранее вполне нормально, начала выходить на перезагрузку при попытке активизировать прикладные программы пользователей. После непродолжительного исследования под подозрением оказался системный файл COMMAND.COM, значительно увеличенный в размерах — примерно на 0,5 Кбайт. Был скопирован "нормальный" файл COMMAND.COM, и программу вновь запустили на выполнение. Каково же было удивление научных сотрудников, когда буквально на глазах файл вырос до прежних размеров! Потребовалось применение специальной программы-отладчика, чтобы в пошаговом режиме убедиться в горькой истине: нарушения в работе ПК вызываются чьим-то злым умыслом, а отнюдь не случайной ошибкой. Выяснилось, что сотни программ в институте инфицированы вирусом, который получил название DOS-62. Вирус запускался программой-носителем и приступал к поиску программы-"жертвы". В случае, если таковая находилась, то с вероятностью семь восьмых она инфицировалась, с вероятностью одна восьмая — модифицировалась так, что дальнейшее ее использование не представлялось возможным. Таким образом, вирус предпринимал усилия, чтобы заразить как можно больше программ и

тем самым обеспечить себе выживаемость. Финал этой истории, к счастью, оптимистичен: была разработана программа ANTIVIRUS, позволяющая проводить надежное диагностирование и лечение IBM PC XT/AT от трех вирусов, распространенных в СССР: DOS-62, "листопад" и "черная дыра".

Описанный выше вирус вполне можно отнести к категории "гуманных". Некоторые же используются в преступных целях — для шантажа и вымогательства крупных денежных сумм. Так, действие вируса, известного под названием "Мозг", заключалось в том, что на экранах дисплеев появлялось следующее сообщение: "Добро пожаловать в долговую тюрьму". Если хотите получить вакцину от этого вируса, обращаться к ..." — далее следовал адрес и телефон "благодетеля", а также цена — 2 тыс. долл.[16].

Известны случаи, когда владельцев компьютерных систем информировали по телефону о том, что к одному из его компьютеров подключена вирусная "бомба замедленного действия" и предлагали за определенную сумму устранить ее, причем сумма достигала сотен тысяч и даже миллионов долларов. Часто владельцы компьютерных систем не решаются сообщить о случаях шантажа в полицию, ведь это показывает, насколько не защищены их компьютеры.

Первое уголовное дело в США по поводу умышленного внесения КВ было начато в 1985 г. Увольнение директора по безопасности компьютерных систем Д.Берлесона обошлось страховой компании ЮСПА энд ИРА дорого: КВ исказил значительное число записей, представляющих собой конфиденциальную информацию. Суд, состоявшийся в октябре 1988 г., приговорил Берлесона к уплате компенсации в размере 12 тыс.долл. или к 10 годам тюремного заключения [14]. В настоящее время в 48 штатах США действуют законы, по которым компьютерные преступления уголовно наказуемы, однако эти законы были приняты до массового распространения "электронных эпидемий". Конечно, законодательство нуждается в существенной доработке (прежде всего это касается СССР), но необходимо учитывать и факт крайне трудного выявления конкретного автора КВ, а тем более доказательство его вины. Этому способствует значительное число модификаций вирусов, различающихся по месту выявления, характеру деструктивных действий и логической схеме функционирования.

По логике функционирования существующие вирусы можно разделить на четыре основных вида: "ловушки", "логические бомбы", "черви" и "троянские кони". Вирусы-"ловушки" используют различного рода ошибки и неточности в ПО для собственных целей. Так, например, при разработке программ часто используется следующий прием: программист указывает точки входа (адрес команды или саму команду, с которой начинается выполнение подпрограммы), служащие для отладки ПО или размещения в некоторой области памяти дополнительного кода. На завершающих этапах разработки ПО эти точки обычно уничтожаются. Однако, если программа насчитывает несколько тысяч операторов и к тому же плохо структурирована, разработчик часто бывает не в состоянии контролировать все точки входа. В этом случае они открывают неограниченный и практически неконтролируемый доступ к любым ресурсам ВС. Места отладочных процедур занимают вирусы-ловушки, выполняющие отнюдь не безобидные действия.

Иначе активизируются "логические бомбы" — вирусные программы, осуществляющие злоумышленные действия при выполнении ряда логических условий. Наиболее распространенный тип таких программ — "бомбы замедленного действия". В этом случае сигналом для начала агрессии может быть определенный этап работы ПК, наступление конкретного времени и даты, результат какого-то случайного события в компьютерной среде, иногда относящегося к достаточно отдален-

ному моменту времени. Особая опасность "логических бомб" заключается в существовании у этих программ определенного "инкубационного периода", в течение которого они стараются заразить многочисленные резервные копии основного ПО.

Программы "черви" маскируются под средства, используемые системными программистами для поиска свободных в данный момент времени вычислительных ресурсов в сети. Получив сигнал о том, что то или иное устройство простаивает, программа-диспетчер на центральной ЭВМ просматривает список задач, ждущих обслуживания от устройств этого типа, и распределяет задачу на соответствующее устройство. В отличие от этих средств "черви", выявив простаивающее устройство, не сообщают об этом программе-диспетчеру, а самовольно его захватывают, заставляя выполнять бесполезную и дорогостоящую работу: распечатывать целые рулоны бумаги, обрабатывать бесконечный циклический участок программы и так далее, тем самым дезорганизуя работу ВС в целом.

Пример программы "троянского коня" уже рассматривался. Вирусы подобного вида, маскирующиеся под обычные прикладные программы пользователей, наиболее распространены в силу простоты их создания и легкости размножения в программной среде.

Все известные к настоящему времени программы-вирусы имеют приблизительно одинаковую структуру. Они состоят из четырех частей. Первая часть представляет собой фрагмент программного кода, с помощью которого вирус попадает в память ЭВМ. Вторая часть обеспечивает копирование вируса на гибкий или жесткий диск, добавляя его к файлам или загрузочному сектору на диске Третья часть описывает условия, при которых вирус активизирует свою деятельность. Наконец, четвертая часть вирусной программы и есть собственно алгоритм ее деструктивных действий.

Исследуем логику работы вируса на примере так называемого Lehigh — вируса, названного так в связи с местом первоначального появления (Lehigh University, Пенсильвания) [17]. Вирус прячется в идеальном с точки зрения возможности размножения файле операционной системы — COMMAND.COM. Этот файл активизируется при вводе всех основных команд ОС — RENAME, DIR, DEL и т.д. Продумано и конкретное место для хранения кода вируса в файле — стековая область, именно благодаря этому инфицированный файл COMMAND.COM не отличается по размерам от обычного. Всякий раз, когда оператор вводит команду DOS, вирус проверяет, есть ли в системе еще неинфицированный файл COMMAND.COM. Если таковой обнаруживается, происходит его заражение и увеличение счетчика числа зараженных дисков. В случае, если значение счетчика достигает четырех, вирус "проявляет себя" — полностью стирает всю информацию на жестком диске. Как мы видим, все четыре этапа работы вируса налицо.

Несколько слов хотелось бы сказать о сложности программ-вирусов. Она колеблется от очень простых (доктор Highland, редактор журнала Computer and Security, разработал вирус, используя лишь инструкции командного файла DOS), до весьма сложных (так называемый Cornell-вирус содержит более 30 тыс. операторов).

По признаку области своего функционирования КВ можно разбить на три группы: поражающие информацию на ПК, инфицирующие большие ЭВМ и дезорганизующие работу вычислительных сетей.

Вирусы первой группы наиболее распространены, это объясняется легкостью копирования ПО на гибких дисках, относительной простотой и дешевизной ПК, отсутствием в большинстве организаций, имеющих ПК, специальных мер по борьбе с "электронной инфекцией". Только за один 1988 г. в организацию "Ассоциация по борьбе с компьютерными вируса-

ми" (США) поступили сообщения о 400 случаях заражения вирусами, которые вывели из строя не менее 90 тыс. ПК [14]. При этом необходимо учитывать, что масса вирусных преступлений просто нигде не фиксируется и не учитывается.

Что касается больших ЭВМ, то инфицирование их вирусом составляет значительно большую трудность, хотя зачастую они являются переносчиками и даже источниками инфекции в составе распределенных компьютерных сетей. Внедрение КВ в ПО больших ЭВМ обычно преследует цель дезорганизации работы крупных вычислительных центров и систем. Так, в ноябре 1988 г. были предприняты две вирусные атаки на компьютерную систему комиссии по атомной энергии США в Ливерморской лаборатории. Чуть позже поступило сообщение о поражении вирусом крупнейшей сети министерства обороны США АРПАНЕТ, объединяющей около 60 тыс. компьютеров на всей территории США. Несмотря на принятые экстренные меры, предотвратить вспышку эпидемии не удалось: вирус проник и в более секретную сеть МИЛНЕТ министерства обороны, которая была снабжена специальными средствами по борьбе с несанкционированным доступом к информации.

Способы борьбы с вирусной эпидемией

Поставщики ПО быстро отреагировали на появление программ, инфицирующих компьютерные системы. Специалисты в области безопасности информации разработали и предложили к продаже серию антивирусных программ, способных подавить или значительно ограничить распространение вирусов определенного типа. К сожалению, подобные "лекарства" обычно ориентированы на лечение уже известных заболеваний, в то время как разработчики программ-вирусов никогда не стоят на месте. В результате эффективность применения антивирусных программ снижается, а число вирусов нового типа стремительно растет.

Растет и спрос на услуги специалистов в области компьютерной безопасности — только в США их стоимость оценивается десятками миллионов долларов. Борьба с электронной эпидемией ведется по трем основным направлениям: аппаратные средства защиты; программные средства защиты; юридические меры.

Аппаратные средства чаще всего реализуют различные криптографические схемы и используются в совокупности со специальными ПО, позволяющим решать специфические задачи борьбы с вирусами: создание графа управления потоком, проверки приоритета программ и т.д. Широкого распространения подобные средства не получили: сказывается их немалая стоимость и влияние на эффективность функционирования ВС.

Программные средства защиты от вирусов можно разделить на две большие группы: предупреждающие внедрение вируса в систему и выявляющие источник инфекции в уже зараженном компьютере. Программы первого типа находятся на резидентных дисках и периодически проверяют систему на наличие в ней вируса.

Проверяются также все подключенные к системе диски, и в случае опасности вирусной атаки выдается предупреждающий сигнал. Прежде всего отслеживаются такие симптомы деятельности вируса, как запись на рабочую программу, блок загрузки диска или системный файл.

Программы второго типа локализуют место внедрения вируса путем прогонки "пустой" системы и выявления изменений в системных файлах. Заинтересованного читателя мы отсылаем к недавнему обзору вирусов и антивирусных программ, опубликованному в журнале "Зарубежная радиоэлектроника" [18], здесь же хотелось бы привести ряд практически ценных советов.

1) Не используйте программ с незарегистрированными авторскими правами. Фирма "Провиденс джор-

нэл" требует, чтобы пользователи загружали свои ПК только с дисков, принадлежащих компании. Служащим "Хьюлетт-Пакард" запрещено использовать на службе ПО без зарегистрированных авторских прав [14].

2) Осуществляйте централизацию закупок ПО согласно заверенному перечню поставок.

3) Активно используйте наклейки запрета записи на гибких дисках — для вирусов типа Lehigh это серьезный барьер!

4) Тщательно инструктируйте пользователей об опасности "электронной эпидемии". Объясните угрозу, исходящую от применения неизвестных программ.

5) Используйте антивирусные программы-вакцины.

6) Контролируйте размеры всех файлов — системных и рабочих. Распечатайте таблицу, содержащую исходную информацию о размерах файлов, и сравнивайте ее с текущей — вирус часто изменяет размеры файлов.

7) Нередко вирус обращается к пользователю с каким-то заявлением или требованием. Осуществляйте просмотр дисков на наличие "странных" текстов типа: "Привет! Я вирус..." и т.п.

Какие действия необходимо предпринять, если КВ все же поразил вашу вычислительную систему?

Вообще говоря, это зависит от того, что собой представляет пораженная ВС и каким образом она была инфицирована. Однако можно дать и некоторые общие рекомендации.

1) Отключите компьютеры от источника питания, это предотвратит дальнейшее поражение и/или повторное инфицирование вирусом.

2) Попытайтесь изолировать вирус, определить логику его работы. Пользуйтесь специальными антивирусными программами.

3) Определите характер и размеры области поражения вирусом: распространился ли он на другие ЭВМ, если ваш ПК подключен к сети ЭВМ.

4) Полностью очистите зараженные диски, которые могут быть восстановлены с помощью дублирующих дисков или лент. Если же в вашей организации не осуществляется регулярной поддержки системы восстановления, то сотрите все подозрительные программы, остальные проверьте на "пустой" системе несколько раз. Иногда приходится жертвовать некоторой информацией для полной уверенности в "выздоровлении" ВС.

5) Установите причину заражения. Помните, вирус никогда не появляется "сам по себе". Проведите тщательный разбор вирусной атаки с сотрудниками вашей организации, вообще больше уделяйте внимания "человеческому фактору".

Итак, вашу ВС поразил вирус. На возвращение ее в рабочее состояние придется потратить немало сил и средств. Кто возместит вашей организации ущерб?

Руководитель специальной группы по изучению компьютерных преступлений, Кирк Тэбби, являющийся также помощником прокурора в Эн-Арборе (шт.Мичиган) заявил: "Уголовное дело можно возбудить всегда, когда существует человек, совершивший его". Незаметное внедрение вируса в ВС является злонамеренным действием, а создание подобной программы — преступлением" [17]. Таким образом, фирма, разрабатывающая и выпускающая ПО, должна нести определенную ответственность за продукт, зараженный вирусом ("VIRUS FREE"). Как уже упоминалось, в ряде стран уголовное законодательство предусматривает ответственность за компьютерные преступления, в том числе и за внедрение вирусов. Однако данные юридические акты направлены против конкретных лиц, внедривших или создавших вирус, а доказать их вину крайне сложно. Какие же меры могут быть приняты против частого лица или фирмы, продавшей вам зараженное ПО? Могут ли они нести какую-либо ответственность?

Джеймс Эйрес, адвокат чикагской фирмы "Нэджи, Коллинз и Лодж", он

"Больные" компьютеры

СИНГАПУР. В прошлую пятницу, 13 июля, компьютеризованный Сингапур нервничал. Владельцы больших ЭВМ и персональных компьютеров опасались атаки компьютерного вируса, получившего название "Пятница, 13-е". И действительно, "болезнь" поразила несколько десятков машин. Однако не успели счастливчики, которых злой рок миновал, свободно вздохнуть, как по стране прокатилось тревожное известие о возможной атаке нового вируса — "Суббота, 14-е". На этот раз опасения оказались напрасными, однако надолго ли?

Сингапур, где ЭВМ являются нормой уже и в детских садах, платит за прогресс возрастающей зависимостью от компьютеров и возможных их "хворей". Поэтому здесь, как и в других развитых странах, так страшатся компьютерных вирусов. Последние, возникая случайно или по воле высокообразованных хулиганов, представляют собой программы-"убийцы", которые, попадая в память ЭВМ, уничтожают или искажают ее содержание. Так, "Пятница, 13-е", проникнув в компьютер, ничем себя не проявляет до ближайшей пятницы, приходящейся на 13-е число, когда он начинает замедлять работу ЭВМ и в конечном счете стирает записанную в ее памяти информацию. Вирус "Суббота, 14-е", как предполагается, родился в Южной Африке, откуда начал бродить по свету. Специалисты полагают, что этот вирус был создан исключительно для того, чтобы досадить тем смекалистым пользователям компьютеров, которые, стремясь избежать атаки "Пятницы, 13-е", накануне роковой даты переводят часы ЭВМ на сутки вперед.

Из "календарных" вирусов Сингапур поразили также "1 апреля" и "Воскресенье". "1 апреля" характерен тем, что на экране ЭВМ сначала появляется послание: "Ха-ха-ха. С 1 апреля у тебя вирус", после чего

(Окончание см. на с. 41)

же представитель юридического колледжа университета De Paul, считает что проблема разрешима несколькими способами [17]:

заключением контракта на законодательной основе между двумя или более организациями;

использованием единого коммерческого кодекса для покупателя и продавца;

принятием договора об устранении последствий возможных вирусных атак.

Главное, что препятствует фактическому внедрению описанных мер, — это непонимание того, что информация давно уже стала продуктом и товаром. А раз это так, к ПО применимы все юридические категории куплие-продажи товаров: коммерческий кодекс, гарантийное обслуживание, санкции за плохое качество и скрытые дефекты и т.д.

Современный мир очень хрупок, взаимосвязан и взаимозависим. В значтельной степени это объясняется широким распространением компьютерных систем управления и связи. Информация, циркулирующая в подобных системах, является критическим элементом, способным вызвать крупномасштабные аварии, военные конфликты, дезорганизацию деятельности научных центров и лабораторий, разорение банков и коммерческих организаций.

Информация может представлять личную, военную, государственную или коммерческую тайну. Наконец, информация стала товаром, который имеет цену, автора, гарантии качества. Миллионы людей участвуют в честном производстве, обмене и распределении этого товара, но находятся и те, кто пытается на этом нагреть руки.

Как же сделать наш компьютерный мир надежным и безопасным? Общество ждет ответа на этот вопрос.

Литература

1. Персональный компьютер: Рабочее место профессионала/Авт. предисл.И.И.Макаров. — М.: Наука, 1989. — 172 с., ил.

2. Becay A. Computer Crime. — Toronto, 1978.

3. Weiss H. Computer Security, an overview Datamation. — 1974. — V.20 — № 1. — P. 42-47.

4. The Computer Law and Security Report. — 1989. — V.5. — № 1. — P.2-5.

5. The Computer Law and Security Report. — 1989. — V.5 — № 2 — P.41.

6. Смид М.Э., Бранстед Д.К. Стандарт шифрования данных: прошлое и будущее// ТИИЭР, 1988. — Т.76. — № 5.

7. Диффи У., Хеллмен М.Э. Защищенность и имитостойкость: введение в криптографию//ТИИЭР, 1979. — Т.67. — № 3.

8. Шеннон К. Теория связи в секретных системах. — В кн.: Работы по теории информации и кибернетике. — М, 1963.

9. Бияшев О.Г., Диев С.И., Размахнин М.К. Основные направления развития и совершенствования криптографического закрытия информации//Зарубежная радиоэлектроника. — 1989. — № 12.

10. Диффи У. Первые десять лет криптографии с открытым ключом/ТИИЭР, 1988. — Т. 76. — № 5.

11. Герасименко В.А., Размахнин М.К., Родионов В.В. Технические средства защиты информации//Зарубежная радиоэлектроника. — 1989. — № 12.

12. Хоффман Л.Дж. Современные методы защиты информации/Пер. с англ. — М.: Сов.радио, 1980.

13. Ahituv N., Lapid Y., Neumann S. Verifying the Authentication of an Informatin System User//Computers and Security. — 1987. — V.6 — P.152-157.

14. Лигская А.В., Миримская О.М. Компьютерный вирус//США: ЭПИ. — 1989. — № 12.

15. Абрамов С.М. и др. Компьютерный вирус//Микропроцессорные средства и системы. — 1989. — № 2.

16. Герасименко В.А. Проблемы защиты данных в системах их обработки//Зарубежная радиоэлектроника. — 1989 — № 12.

17. The Computer Law and Security Report. — 1989. — V.5. — № 1. — P.18-21.

18. Агеев А.С. Компьютерные вирусы и безопасность информации//Зарубежная радиоэлектроника. — 1989. — № 12.

О вирусах, червях, троянцах и бомбах

Как и биологические вирусы, поражающие живые клетки, компьютерные вирусы содержат набор кодовых команд, которые позволяют им вторгаться в главные вычислительные машины, размножаться и поражать новые компьютеры. Изощренные вирусы могут распространяться, будучи необнаруженными в течение длительного времени, ожидая сигнала к началу разрушения данных. Сигналы могут быть разными. Например, один из известных вирусов был запрограммирован на внесение хаоса по пятницам, приходящимся на 13 число, другой начинал свою деятельность после того, как воспроизводил четыре себе подобных вируса.

Но одно, общее для всех вирусов, качество заключается в том, что все они являются паразитами, так как прикрепляются к другим программам. Поэтому знаменитый вирус, поразивший Internet, строго говоря, не является вирусом. Эксперты утверждают, что это был червь — программа, которая повторно себя дублирует, но является изолированной. Троянские программы, названные в честь знаменитого троянского коня в древнегреческой мифологии, — это программы, которые кажутся безвредными, но содержат вредительские части. "Бомбы" похожи на "троянцев", но они не привносятся снаружи, а скрываются в обычных программах. Раздраженный служащий может, например, установить "бомбу с часовым механизмом", запрограммированную на "взрыв" через месяц.

Что делает вирус, когда он попадает в компьютер? Он может прикрепиться к boot-сектору, ОС или выполняемой программе. Boot — это программа запуска, которая загружается перед любой другой программой. Она подготавливает к работе ОС и дает возможность пользователю работать с другими программными средствами, а также с такими устройствами, как принтеры или модемы.

Boot-вирус обычно заменяет первую дорожку диска на часть собственного тела. Свою оставшуюся часть он прячет вместе с реальным boot-сектором в каком-то другом секторе диска — область, которую он помечает как плохой сектор. Вирус управляет машиной, пока она включена. Затем он позволяет первоначальному boot-сектору выполнить свои функции. Как только boot-вирус попадает в машину, он копируется на первый сектор другого диска, который введен в компьютер.

Вирусы могут также заражать программы внутри ОС, вызывая самые разные проблемы. Вирусы могут инфицировать файлы, к которым имеется доступ, замедлять функции компьютера или изменять сообщения, появляющиеся на экране.

Наиболее распространенные вирусы поражают прикладные программы: текстовые процессоры, крупноформатные таблицы, игры, утилиты. Когда это сделано, вирусы могут распространяться на другие компьютеры. Многие вирусы проверяют: заражена ли программа, и если файл уже инфицирован, уклоняются от его повторного заражения. Это объясняется тем, что в противном случае программа станет слишком большой, не поместится в память и вирус будет обнаружен.

Некоторые вирусы относительно безопасны. Так, вирус поразивший компьютеры "Макинтош" 2-го марта 1988 г., в канун представления Мак 11, выдал на экран всех дисплеев следующее послание: "Ричард Брендоу и его персонал рады возможности передать свое Послание Мира всем пользователям компьютеров Макинтош".

Однако большинство вирусов вызывают тяжелые последствия. Одними из весьма неприятных вирусов в настоящее время являются те, которые вызывают аварийный останов, в результате чего теряются данные. Но наиболее коварные из нового поколения вирусов изменяют данные, не уничтожая их. Вирусы достигли уже Советского Союза. В Институте программных систем описан вирус "Капающие слезы" (в США он называется "Каскад")*. Другой вирус, появившийся в СССР, называется "Черная дыра" (американское название Israeli). Он тратит процессорное время, выполняя ничего не значащие операции. Вирус также выдает в углу экрана темное пятно. Отсюда и его название. Но не все страны называют вирусы в соответствии с их поведением, местом или происхождением. В Великобритании, например, вирусы называют по их размеру, например "1808"(байт).

ЦРУ и Управление национальной безопасности исследовали возможность заражения вирусом компьютерных систем других стран. Многие компании мира ведут исследования и экспериментируют с вирусами и средствами защиты от них, но предпочитают молчать об этом. Это затрудняет определение количества вирусных эпидемий. Промышленная ассоциация компьютерных вирусов (CVIA), представляющая ряд компаний, продающих антивирусные программы, сообщила, что в прошлом году вирусы поразили более 90 тыс. ПК. CVIA утверждает также, что 90% компаний, пораженных вирусом, вновь инфицируется в течение месяца, заражаясь с дублируемых дисков.

Однако о серьезности проблемы вирусов ведется много споров. Некоторые ученые считают, что эта проблема сильно преувеличена. Другие же, наоборот, предостерегают от ее недооценки. Но без сомнения, все те, кто регулярно обменивается программами, должны принимать меры предосторожности против катастрофической потери данных.

Самый простой путь заражения вирусом своих программ — это использование пораженного вирусом диска, одолженного, например, у товарища. Поэтому очень важно знать происхождение используемой программы. Пользователи, заказывающие диски у фирмы, должны быть уверены, что компания получает программы непосредственно от авторов и проверяет диски перед их распространением.

Особенно важно не использовать пиратские программы. Но и коммерческие программы могут быть поражены вирусом. Один из вероятных путей заражения — это копирование программы с компьютерной информационной панели. В Нью-Йорке существуют сотни этих систем, и многие операторы, работающие на них, не проверяют программы на наличие вирусов.

Вирусы могут быть также замаскированы под антивирусные программы.

Как специалисты по борьбе с вирусами борются с ними? По словам одного из сотрудников Apple, практически невозможно проследить обратное распространение вируса и найти источник его происхождения. Например, специалисты, искавшие источник нашумевшего вируса Internet, смогли добраться до причины только потому, что ими был обнаружен в файле злоумышленника список паролей, используемых для вторжения в систему, и ранняя версия червя, который впоследствии засорил группы блоков памяти компьютеров в сети.

* Вирус проявляется в том, что буквы начинают "падать" и с треском "сбивать" все нижестоящие, при этом блокируется клавиатура.

Одна из наибольших сложностей в поиске источника вируса заключается в том, что программы пишутся с использованием многих разных языков и компилируются разными методами. При поиске источника вируса приходится декомпилировать программу, а это аналогично использованию одного словаря для перевода с одного языка на другой и иного словаря для обратного перевода.

Многие исследователи изучают вирус, давая ему возможность действовать в изолированной системе. Для этого создают локальную сеть и, находясь, например, в конференц-зале, изучают шаг за шагом поведение вируса.

Для того чтобы защитить себя от вируса, очень важно часто пользоваться копированием файлов на резервные диски. Это позволяет стирать зараженные файлы и заменять их на чистые в случае попадания вируса. Конечно, "тихие" вирусы могут попасть и на эти диски. Поэтому производители начали выпускать антивирусные программные и аппаратные средства.

Zeus Corp. из Акрона, штат Огайо, сделала "Иммунетек PC" — съемную схемную плату, проводящую проверку на наличие вирусов в IBM-совместимых компьютерах. Другая компания "Американ компьютер секьюрити индистриз" из Нешвила утверждает даже, что сделала антивирусный компьютер, названный "Иммун систем". Он, в частности, снабжен аппаратурой, предотвращающей изменения в ОС.

Развиваются также и антивирусные программные средства. Многие такие программы названы в соответствии с медицинской терминологией: "Вакцина", "Антитоксин", "Интерферон" и т.д. Одна из компаний, продающих антивирусные программы, даже создала Центр по контролю за компьютерными болезнями.

Существуют 3 вида антивирусных программ.

Первые — это программы-фильтрации, создаваемые для предотвращения заражения. Они находятся в памяти компьютера все время, контролируют операции и наблюдают за сигналами и за попытками вируса просочиться. Если фильтр опознает аномальное поведение, текстовой процессор может, например, заморозить систему и выдать мигающее предупреждение. Однако появляющиеся новые вирусы могут "одурачить" фильтры. Кроме того, фильтры бывают слишком обременительными, так как могут постоянно прерывать работу пользователя ложными тревогами.

Второй вид программ — вирус-детекторы или программы-ревизоры. Они "фотографируют" состояние системы и периодически сравнивают его с этим снимком. Если что-то меняется, они выдают сигнал тревоги. Другие программы-ревизоры основаны на подсчете контрольных сумм, позволяющем с помощью математических формул определить целостность программ и данных. Одно из неудобств этих программ заключается в том, что они едят процессорное время, так как периодически останавливаются для проведения вычислений.

Третий вид программ — это программы-фаги. Они обучены искоренять после распознавания простые вирусы. Но они хороши лишь для обнаружения старых вирусов и могут оказаться непригодными для новых модификаций.

Фирма RSA продает системы кодирования, основанные на технологии, разработанной в Массачусетсском технологическом институте в конце 70-х гг. Эта фирма недавно представила продукт, названный RSA Sign, позволяющий издателям программных средств добавлять цифровую сигнатуру к программам. Но кодирование бесполезно, если ОС компьютера недостаточно защищена. Любой план безопасности, который не адресуется сети в целом — аппаратным или программным средствам, — будет в конечном счете обречен на неудачу.

Другие эксперты по безопасности рассчитывают на средства ограничения доступа к компьютерным фай-

лам. Многие компании уже требуют от пользователей применять определенные ключи в дополнение к паролю. Но и это не сможет удержать злоумышленников, имеющих доступ к файлам, от установки бомб.

Одна из систем, ограничивающих права пользователей, создана М.Рабином, профессором-компьютерщиком Гарварда, и Д.Тугаром из университета Карнеги-Меллона (г.Питтсбург). Это набор сложных математических процессов, которые определяют пользователей по их роли в той или иной работе и отсекают от файлов, не имеющих к ней отношения.

Пока разработка систем безопасности делает робкие шаги, некоторые официальные лица пытаются залатать дыры с помощью нового законодательства. В результате в палату представителей поступили два антивирусных законопроекта.

Тем временем организация, называющаяся "Профессионалы-компьютерщики за социальную ответственность", пишет код этики. Предлагается также награда всякому, кто вычислит написавшего вирус. Кроме того, в качестве дополнения к программам предлагается использовать призыв следующего содержания: "У вас есть талант, чтобы сделать что-то полезное в жизни. То, что вы делаете, вредит промышленности и обществу, которое радо принять вас и ваш талант с распростертыми объятиями. Удовольствие, которое вы получите от сотрудничества с нами, намного превзойдет то, которое вы получите при нанесении вреда ни в чем не повинным людям. Остановитесь!"

Ниже приводится краткое описание некоторых из известных вирусов.

Pakistani brain (Пакистанский мозг)**

Заменяет первоначальный boot-сектор на собственное тело, передвигает первоначальный сектор на другое место. Добавляет 7 секторов, которые содержат остаток вируса. Сигнализирует обо всех модифицированных секторах как о бесполезных с целью защитить себя. Дублируется на все пораженные загрузочные гибкие диски.

Симптомы: замедление последовательности повторной загрузки, чрезмерная работа гибкого диска при выполнении простых задач. Аварийный останов программ для некоторых ОС.

Alameda (Аламеда)

Заменяет первоначальный boot-сектор на свое тело. Прячет оригинальный boot-сектор в первом свободном кластере. Не отмечает этот кластер как сбойный, оставляет его доступным для распределения. В случае перезаписи содержимого этого кластера становится невозможной перегрузка системы.

Симптомы: медленная последовательность загрузки, аварийный останов, потеря данных.

Israeli (Черная пятница)

Заражает любые программы типа Com или Exe. Увеличивается размер программы на 1,8 кбайт. Инфицируемые программы модифицируются и становятся ОЗУ-резидентными. Программы инфицируются, когда выполняются в инфицируемой системе; гибкие или жесткие диски могут инфицироваться.

Симптомы: общее замедление работы системы, уничтожение программы 13-го числа, если оно приходится на пятницу. Файлы типа Exe продолжают расти до тех пор, пока не станут столь большими, что их нельзя будет выполнять. Возможно уменьшение системной памяти.

nVir

Появляется во *многих вариациях*, всегда с различными особенностями;

** Так как авторами вируса являются молодые пакистанцы, а вирус присваивает дискетам имя *Brain*, вирус часто называют "Душманские мозги".

публикация исходного кода для этого вируса определяет его широкие вариации; кодовый ресурс содержится в прикладной программе; если система заражена, любая прикладная *задача* инфицирована.

Симптомы: сильно различаются из-за большого числа вариаций; аварийный останов; слышен гудок, когда открыта прикладная задача; может передаваться сообщение "без паники"; исчезновение файлов.

Примечание: nViR особенно опасен и может заражать все программы внутри системы в течение нескольких минут.

Lehigh

Заражает команды, файлы типа com; увеличивает размер файла примерно на 20 байт; изменяет дату и время; начинает действовать после 4 инфекций; разрушает все системные данные.

Симптомы: изменение размера команд; потеря всех данных.

Примечание: из-за короткого периода активности шансы обнаружения вируса до уничтожения невелики.

(автор статьи By Dawn Stover)
Popular Science9.89,
с. 59-62,104,110.

Теория рынка служит распределению вычислений

Компьютерный вирус Spawn, в основе которого лежат идеи Адама Смита, является не только средством научных экспериментов в экономике, но и начинает находить более широкое применение.

Spawn — это "домашний" компьютерный вирус, созданный в лаборатории Центра Palo Alto Research Center, (PARC) фирмы "Ксерокс". Это полезный вирус, способный разветвляться внутри сети и заражать машины такой "болезнью", при которой они начинают все вместе производительно работать без помощи главного планирующего органа. На создание такого вируса разработчиков натолкнула мысль о том, что мощные и скоростные аппаратные средства часто неэффективно взаимодействуют, имеют узкие места, ограничивающие интенсивность работы, или даже вынуждают машины простаивать. Специалисты Центра PARC решили использовать этот бездействующий потенциал.

В сущности, их идея основана на создании автоматизированной компьютерной сети, загрузка которой производится по принципам рыночных отношений, главным из которых является соотношение между спросом и предложением.

Система уже была опробована на решении двух задач: формировании больших сложных документов и вычислениях Монте-Карло. Система могла также дать хорошие результаты при факторизации больших чисел, криптографии и ряде других задач, которые нетрудно разбить на составные части. Ключевым моментом в решении таких задач является выяснение, как при этом происходит "самоорганизация" компьютеров.

На первый взгляд наиболее очевидным представляется решение о создании какого-то центрального планирующего механизма, использующего один главный компьютер, который давал бы команды всем подчиненным машинам. Но когда компьютерные системы объединены именно так, их взаимодействие оказывается малоэффективным. Машины тратят на связь с главным компьютером и координацию своих действий так много времени, что его остается слишком мало на непосредственную работу. Идея специалистов фирмы "Ксерокс" заключается в том, чтобы заставить компьютеры взаимодействовать друг с другом без помощи централизованного планирования. В области "распределенных" вычислений это становится самым важным результатом для компьютерной науки в целом.

Вспомним Адама Смита и его теорию рынка. "Невидимая рука" спроса и предложения позволяет координировать экономическую деятельность без централизованного плани-

рования. Эту теорию можно аналогично использовать и для координации работы компьютерной сети.

Spawn — не первая программа, основанная на этой идее. В начале 80-х гг. в Массачусетсском технологическом институте была разработана система "Энтерпрайс".

"Для того чтобы увидеть, как она работает, — говорит руководитель группы Хуберман, — представьте, что вы хотите выполнить большое вычисление Монте-Карло. Сидя за своей рабочей станцией, вы даете программе Spawn проектный "бюджет", имеющий приоритетный уровень, измеряемый в долларах (в первой системе в качестве "долларов" выступали опознавательные знаки, используемые самими компьютерами). Но в работающих системах они могут легко представлять реальные деньги. Затем, когда задача сформирована, вы просто даете Spawn команду действовать. Пока она работает, вам незачем наблюдать; вы можете, например, писать доклад в другом окне экрана или выпить чашечку кофе. Тем временем программа разбивает первоначальную задачу на части и размножает ее на серии независимых вычислений (отсюда и название: Spawn — размножение), каждое со своим бюджетом. Эти субпроцессы, в свою очередь, будут посланы по сети для нахождения необходимого времени и получения места для выполнения своей работы. Эти образовавшиеся субпроцессы не просто вторгаются в компьютеры, а следуют протоколу рынка. Прежде чем они куда-то пойдут, будут посланы предложения с предполагаемой продажной ценой. Будет предложено купить время обработки блоками по 60 с.

Одновременно каждая используемая машина в сети передает свое предложение продать столько времени, сколько она считает возможным освободить. Так же как на экономическом рынке у людей происходит соглашение в цене, и выигравшие субпроцессы поступают туда, где выделено время. Если работа субпроцесса слишком дорого ценится и у него еще по-прежнему остались деньги, он может размножиться на новые субпроцессы и начать новый этап предложения цены.

Если вы единственный человек, пытающийся использовать Spawn, то ясно, что ни один из актов купли-продажи не вызовет проблем. Но что будет, если кто-то захочет запустить свой проект бюджета Spawn так, чтобы вы не знали об этом? В этом случае представьте, что вы сами хотели бы начать еще несколько новых вычислений, перед тем как закончатся первые. Механизм рынка будет продолжать проводить эффективное распределение ресурсов независимо от того, сколько пользователей предлагает цену.

Эксперименты со Spawn, проводящиеся на рабочих станциях в Центре PARC, убедили, что автоматизированный рынок ведет себя так, как и предполагалось: чем больше субпроцессов предлагает цену за компьютерное время, тем выше эта цена. Таким образом, ресурсы автоматически распределяются на процессы с более высоким приоритетом. Если, например, один из субпроцессов выходит на рынок с большим количеством денег, предлагаемая цена сразу подскакивает и процессы с низким приоритетом сразу проигрывают.

Такой автоматизированный рынок достаточно эффективен: сеть в целом тратит менее 10% времени на формирование цены, оставляя 90% на непосредственно полезную работу.

Конечно, во всем этом есть определенные опасности. Spawn существует в лаборатории менее года, и "Ксерокс" пока не стремится сделать из него готовый товар. В настоящее время Spawn представляет собой программный эквивалент физической лаборатории, сплошь и рядом усеянной проводами.

Очень важным в использовании Spawn является вопрос безопасности. "Сейчас Spawn находится в дружественной среде пользователей", — говорит Хуберман, — где все знают

друг друга. Но практическая система должна содержать строгие средства защиты, ограждающие пользователя от вторжения в его работу злоумышленника.

Такая система должна иметь защиту от ошибок в субпроцессах Spawn, приводящих к случайному разрушению программных средств главного компьютера".

Пока рано рассуждать, куда может привести развитие средств подобных Spawn. Сейчас Spawn находится в "сыром" виде, и пользователи вынуждены использовать громозкие команды для приведения его в действие. Однако один из разработчиков Spawn К.Уальдспургер работает над новым языком, который будет приспособлен к распределенным вычислениям в стиле Spawn. Язык, названный Аргус, позволит программистам связывать прикладную задачу со Spawn абсолютно ясным путем: все, что пользователь будет видеть на экране, — это сами прикладные задачи. Человек не будет знать и заботиться о том, задача какой машины в настоящее время выполняется. "Фактически, — говорит Хуберман, — вышеописанный подход — это лишь одна ступень на пути к высокоскоростным национальным сетям, планируемым сейчас Национальным научным фондом и другими организациями. Если сеть будет содержать Spawn или что-то аналогичное, тогда любой настольный ПК будет иметь ту же мощность, что и суперкомпьютер, при условии, что последний будет входить в сеть, а пользователь настольного персонального компьютера будет готов платить за время.

Сейчас группа Центра PARC начала использовать Spawn в своих практических интересах. Разрабатываются новые виды компьютерных моделей для экономики и экологии. Сам Spawn появился в результате попыток понять динамику поведения больших систем конкурентов, как, например, на рынке товаров. В свою очередь эта работа является частью более широких работ физиков, биологов, компьютерщиков и экономистов, изучающих то, что некоторые исследователи называют "возникающие права сложных систем".

"Например, — говорит Хуберман, — Spawn может быть использован для выяснения, что случится с равновесием рынка, если каждый агент будет пытаться предугадать действия конкурентов. Предшествующие работы Центра PARC указывают на то, что это может носить дестабилизирующий характер. Так ли это?

Подводя итог заметим, что сейчас рано говорить, куда Spawn в действительности приведет. Но некоторые экономисты и промышленники сходятся во мнении, что это интригующее начало.

Science News T244, 14.04.89, с.145-146.

БК-ЗА-РОГА

М.Л.Суяргулов

Интерес к БК затухает

Интерес к БК-0010 затухает и связано это в первую очередь с неудачной внутренней организацией самой БК. Имея такой мощный процессор, как К1801ВМ1, компьютер обладает чрезвычайно скромными возможностями. Используя системный разъем БК, можно радикально изменить архитектуру компьютера. Например, расширить ОЗУ. Интерес к БК можно поднять, сделав из данного компьютера удобное инструментальное средство для решения различных задач. Это могут сделать внешние устройства и программное обеспечение к ним. Основное достоинство БК — это низкая цена. Внешние блоки для БК также не должны быть дорогими.

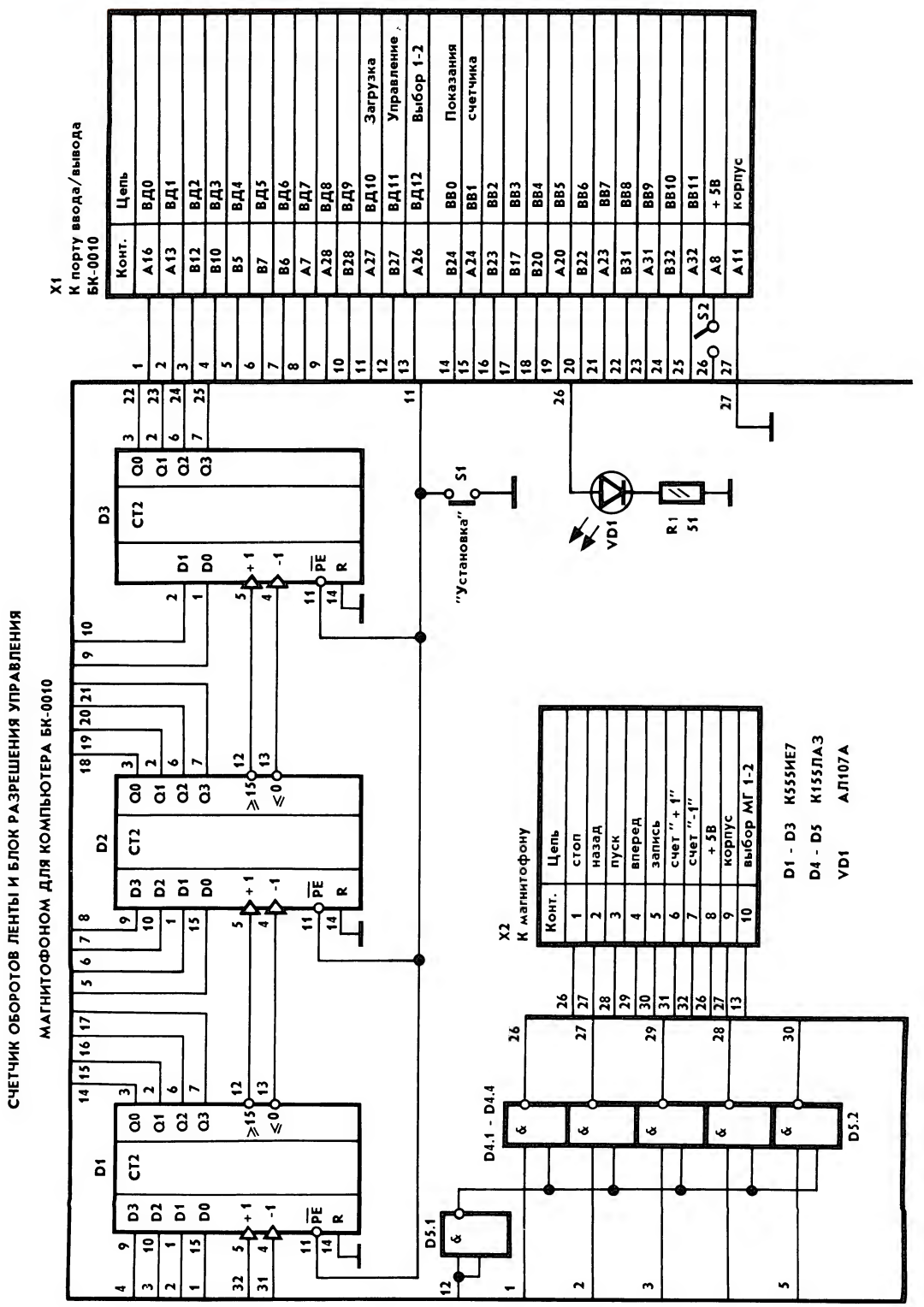
При подключении к БК нескольких устройств возникает проблема их коммутации. т.е. подключения к порту ввода-вывода работающего в данный момент устройства. Одновременно должна обеспечиваться работа каждого устройства без изменения его схемы и программы. Данную проблему можно решить, выделив три старших бита порта вывода для системных целей и не использовать их для работы внешних устройств. Эти три бита должны использоваться как своего рода шина кода устройства, которое работает с портом в данный момент. Эти биты должны подаваться либо на специальное устройство коммутации внешних устройств, либо использоваться в самом внешнем устройстве как разрешающие биты для работы данного устройства с портом БК. Этими тремя битами можно закодировать семь внешних устройств. На мой взгляд, коды 100, 010 и 001 нужно зарезервировать соответственно за принтером, джойстиком и счетчиком для управления магнитофоном.

Конструкция блока коммутации независимо от того, где он находится: в самом устройстве или составляет отдельный блок, будет зависеть от принятого протокола обмена между портом и устройством. Возможны два варианта: код устройства подается на шину кода только в начале обмена для подключения нужного устройства и код остается на шине в течение всего времени обмена.

Теперь о счетчике для управления магнитофоном. Предлагаемое устройство представляет собой реверсивный 12-битный счетчик с инверсной логикой, с разрешением загрузки начального значения и блок разрешения подачи управляющего кода на магнитофон.

Устройство подключается к порту БК через разъем X1. Биты порта вывода ВД0-ВД9 используются для задания начального значения счетчика. При задании начального значения недостающие два бита счетчика заполняются инверсными нулями. Биты ВД0-ВД4 одновременно используются для задания управляющих кодов магнитофона. Бит ВД10 порта вывода используется как бит разрешения загрузки начального значения из порта вывода в регистр счетчика. Бит ВД11 используется для разрешения передачи управляющего кода на магнитофон.

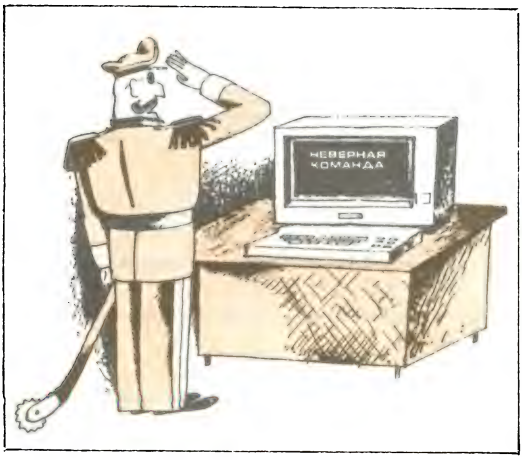
Для упрощения схемы и уменьшения потребления электроэнергии от блока питания блок разрешения подачи управляющего кода на магнитофон собран всего на двух микросхемах К155ЛА3 без применения дополнительных инверторов. Выход управляющего сигнала с блока разрешения должен соответствовать логике порта БК, т.е. должен быть инверсным. Код управления — это такой код, который обеспечивает на выходе блока разрешения управления вывод логической единицы по нужному каналу управления. Например, для передачи логической еди-


СЧЕТЧИК ОБОРОТОВ ЛЕНТЫ И БЛОК РАЗРЕШЕНИЯ УПРАВЛЕНИЯ МАГНИТОФОНОМ ДЛЯ КОМПЬЮТЕРА БК-0010
X1
К порту ввода/вывода БК-0010
Конт. Цепь
A16 ВД0
A13 ВД1
B12 ВД2
B10 ВД3
B5 ВД4
B7 ВД5
B6 ВД6
A7 ВД7
A28 ВД8
B28 ВД9
A27 ВД10 Загрузка
B27 ВД11 Управление
A26 ВД12 Выбор 1-2
B24 ВВ0 Показания
A24 ВВ1 счетчика
B23 ВВ2
B17 ВВ3
B20 ВВ4
A20 ВВ5
B22 ВВ6
A23 ВВ7
B31 ВВ8
A31 ВВ9
B32 ВВ10
A32 ВВ11
A8 +5В
A11 корпус
S2
S1
"Установка"
VD1
R1 51
D1
D2
D3
CT2
D4.1 - D4.4
D5.1
D5.2
X2
К магнитофону
Конт. Цепь
1 стоп
2 назад
3 пуск
4 вперед
5 запись
6 счет "+1"
7 счет "-1"
8 +5В
9 корпус
10 выбор МГ 1-2
D1 - D3 К555ИЕ7
D4 - D5 К155ЛА3
VD1 АЛ107А

ницы по первому каналу "стоп" на порт необходимо подать значение 0000100000011110 двоичное или 4036 восмеричное, где единица в 11-м разряде нужна для разрешения передачи кода в разрядах 0 — 5 порта вывода на выход блока разрешения, а само значение пятизначного кода инвертировано. Для подачи логических единиц по пяти каналам управления нужно применять коды 4036, 4035, 4033, 4027, 4017. Для включения режима "запись" логические единицы необходимо подать одновременно по каналам "пуск" и "запись", поэтому управляющий код режима 4013, а не 4017. При разработке программного обеспечения для счетчика данные коды лучше хранить в отдельном массиве. Это обеспечит легкую адаптацию программ в случае изменения схемы блока разрешения управления магнитофоном.

Порт ввода-вывода БК имеет инверсную логику. Инверсный режим работы микросхемы К555ИЕ7 обеспечивается подачей счета " + 1" на вход микросхемы "-1" и загрузкой в регистр счетчика исходного инверсного значения с порта БК.

Магнитофон подключается к счетчику через разъем X2. Контакты 1 — 5 разъема используются для передачи на магнитофон кода включения одного из пяти режимов работы: "стоп", "назад", "пуск", "вперед", "запись". На контакты 6 и 7 с блока формирования счетных импульсов магнитофона на счетчик должны поступать короткие счетные импульсы отрицательной полярности. Сам блок формирования счетных импульсов не регламентируется. Оговаривается только то, что при движении ленты вперед импульсы должны поступать по каналу счет " + 1", а при движении ленты назад — на канал счет "-1". ребезг импульса недопустим, поэтому при применении геркона в качестве датчика его дребезг нужно отсечь. Как унисерсальную и не зависящую от типа магнитофона, можно предложить схему формирователя счетных импульсов из счетчика расхода ленты, опубликованную в журнале "Радио" № 8 за 1984 г. В этом случае рекомендуется на ролик механического счетчика оборотов ленты надеть полый цилиндр с прорезью.



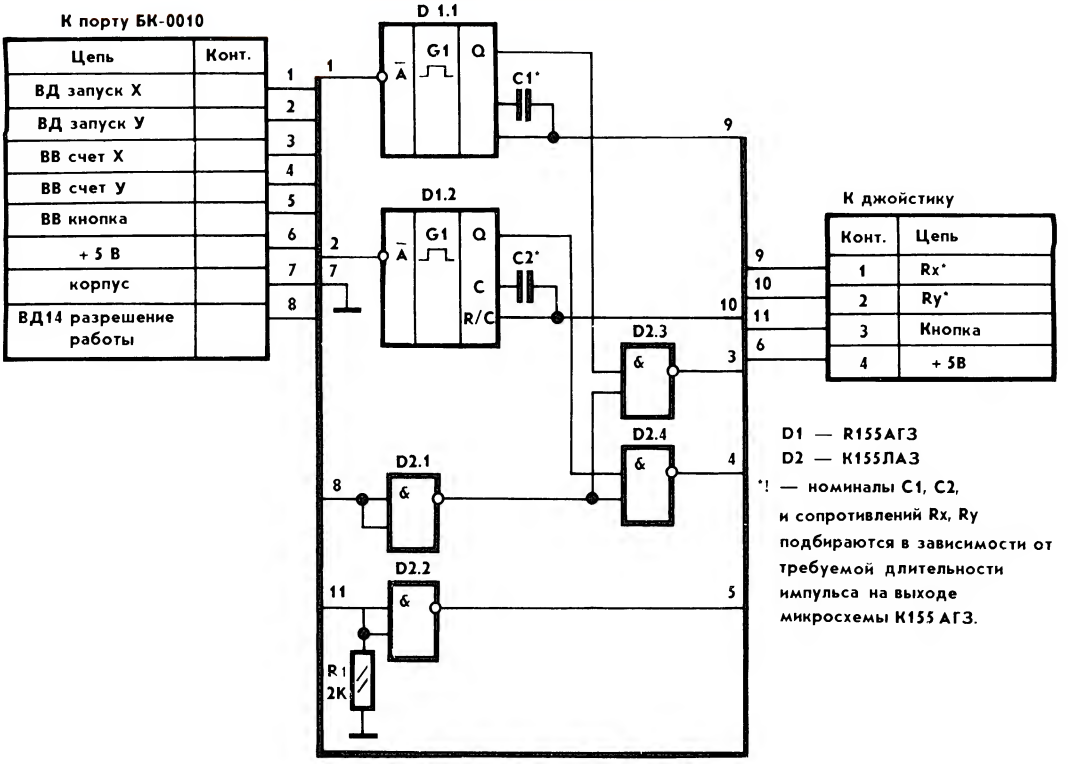
Контакт 10 разъема X2 передает магнитофону бит ВД12 с порта вывода. Этот бит может использоваться для организации совместной работы двух управляемых магнитофонов. Для этого к разъему X2 необходимо подключить блок коммутации на 7 каналов (5 каналов вывода и 2 канала ввода информации в счетчик). При этом сигнал с контакта 10 разъема X2 должен использоваться как сигнал переключения коммутатора.

Вопрос о сопряжении блока разрешения управления магнитофоном с самим магнитофоном или, точнее, с блоком автоматики и управления магнитофоном, решается в зависимости от конструкции магнитофона. Наиболее просто сопрягается с компьютером магнитофон-приставка ОРЕЛЬ-101. Для их сопряжения достаточно подать на вход дистанционного управления управляющие сигналы с выхода блока разрешения: контакты 1-5 разъема X2.

Вся схема в собранном виде легко помещается в стандартном корпусе из-под МСТД. Еще остается место для 4-5 микросхем. Предложения об использовании остающегося пространства позже.

В настоящее время для работы с таким счетчиком имеется только одна

СХЕМА ПРОПОРЦИОНАЛЬНОГО ДЖОЙСТИКА

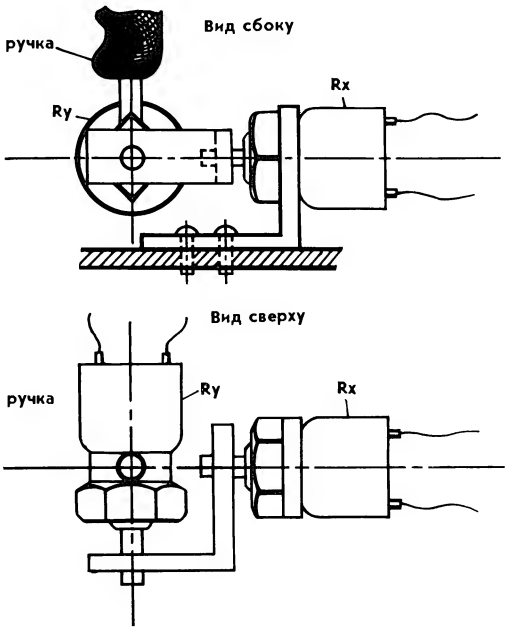


программа. Это начальный загрузчик файлов LOADER. Данная программа позволяет загружать один из тридцати четырех файлов, записанных на данной кассете. Прототип программы — Norton Commander фирмы IBM. От пользователя требуется только вставить кассету, отмотать ленту в начало, так как данная программа должна находиться в начале кассеты, и загрузить файл. Программа сама запустится и выведет на экран директорий данной кассеты. Клавишами "курсор вверх" и "курсор вниз" пользователь выбирает файл и нажимает "ввод". После чего программа отмотает ленту к началу выбранного файла, включит магнитофон на чтение, загрузит и запустит выбранный файл. Помимо этого, программа позволяет составлять директорий новой кассеты и дополнять имеющийся директорий в автоматическом режиме, редактировать записи директория, управлять магнитофоном с клавиатуры компьютера, сохранять всю систему с новым директорием на ленте. На всех этапах работы можно получить исчерпывающую подсказку. Для управления режимами, помимо алфавитных клавиш, можно использовать функциональные ключи.

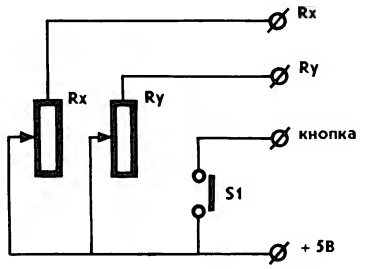
Конечной целью создания данного счетчика является полная автоматизация обмена с магнитофоном, т.е. создание полной файловой системы, позволяющей не только читать, но и записывать файлы, отвечающей за распределение ленты и за размещение файлов на ленте. Но данный счетчик построен так, что он может считать любую информацию, которая в соответствующем виде подается на вход счетчика. Счетчик может быть использован для организации встроенных часов, как счетчик различных процессов, например, для управления станком по намотке радиокатушек.

Как использовать остающееся место в блоке счетчика? Я предлагаю разместить там электронную часть пропорционального джойстика. Предлагаю схему джойстика с разре-

МЕХАНИЧЕСКАЯ ЧАСТЬ ПРОПОРЦИОНАЛЬНОГО ДЖОЙСТИКА



Электрическая схема



шением работы по биту ВД14. Джойстик построен на микросхеме К155АГ3. Данная схема отличается тем, что имеет блок разрешения передачи данных с джойстика на порт ввода БК. Механико-электрическая схема состоит из двух потенциометров, связанных в карданову пару уголком, и кнопки выбора. К ней идут от электронной части всего четыре провода. Для работы джойстика используются два бита порта вывода и три бита порта ввода. Если учесть, что три бита порта вывода зарезервированы, а все биты порта ввода свободны, то одновременно с БК могут работать до пяти таких джойстиков. В корпусе блока счетчика и управления магнитофоном может разместиться электронная часть двух джойстиков. Блок разрешения предлагаемого джойстика следит только за битом ВД14. Если предусмотрена одновременная работа с портом устройств с кодами 011 или 110, необходимо организовать слежение за битами ВД13 и ВД15 шины кода устройства.

Какие возможности открывает использование пропорционального джойстика? Главное приемущество — джойстик позволяет определять не только направление отклонения его ручки, но и величину этого отклонения. Точность работы джойстика зависит от диапазона изменения длительности импульса на выходе джойстика, точнее, от числа циклов суммирования при обработке обращения к одному из измерений джойстика. Если при использовании джойстика для игровых программ достаточно, скажем, пяти-шести градаций скорости управляемого объекта, то диапазон изменения импульсов должен быть в пределах 20/30 циклов; и при использования электронной части джойстика для обработки координатного планшета в цветном режиме монитора 256x256 точек необходим диапазон изменения длины импульса минимум 512 циклов. Вместо потенциометров к электронной части джойстика можно подключить любой резистор, например фото- или термо. Если к свободным выходам порта вывода подключить блок управления устройства, изменяющего состояния измеряемой величины, то можно организовать систему автоматического управления и регулирования.

Таким образом, возможности данной схемы не ограничиваются названием "джойстик". Величины конденсаторов и сопротивлений я не регламентирую. Их величины зависят от области применения данной схемы. Еще раз повторяю, что первая реализация пропорционального джойстика была выполнена кооперативом "Амитон" из Ленинграда. Кооператив распространял две свои программы, одна из которых ПИЛОТ, и ряд адаптированных программ для этого джойстика.

А.М.Надежин

SOS2 — программа спасения файлов с ошибками чтения

В четвертом выпуске серии "Вычислительная техника и ее применение" за этот год была опубликована статья Л.Н.Жарикова о работе БК с магнитофоном, в которой автор, в частности, обращался к читателям с предложением разработать простую программу в машинных кодах, блокирующую возникновение ошибки контрольной суммы файла. Однако при чтении почти всегда испорченным оказывается не только то место файла, где произошла ошибка (дефект магнитной ленты, помеха при записи), но и вся последующая часть файла. Поэтому программа, блокирующая ошибки контрольной суммы, смогла бы спасти только участок от начала файла до первой ошибки, и то лишь в случае успешного считывания заголовка. Поэтому в программе для спасения нечитающихся файлов необходимо использовать другой алгоритм чтения, чем тот, который используется в драйвере магнитофона БК.

Первой такой программой была программа ЧИТМАГ, появившаяся в Москве в начале 1989 года. ЧИТМАГ позволяет считывать с магнитофона любой участок текстового файла длиной 2000 байт и тут же выводит на экран всю символьную информацию, находящуюся в этом участке. К недостаткам программы ЧИТМАГ можно отнести то, что она работает только с блоками по 2000 байт и не позволяет записывать на магнитофон считанные участки, поэтому единственный способ сохранить спасенную информацию — переписать текст с экрана на бумагу и ввести его с помощью текстового редактора.

Для того чтобы избавить пользователя от такой рутинной работы, в начале 1990 г. мной была написана программа SOS, использующая алгоритм чтения программы ЧИТМАГ и имеющая широкие сервисные возможности, устраняющие недостатки ЧИТМАГа. Вашему вниманию предлагается новая версия программы — SOS2. Она позволяет считывать любые участки файлов длиной до 35 000 байт, визуально контролировать ход чтения (файл считывается в экранную область ОЗУ), просматривать считанный текстовый файл на экране, записывать считанный файл на магнитофон под любым именем.

Программа SOS2 написана на языке ассемблера с помощью турбосистемы программирования на языке ассемблера TURBO2. Приведенный листинг в машинных кодах можно ввести в память БК, руководствуясь методикой, подробно описанной в статье Д.Ю.Усенкова (Вычислительная техника и ее применение. — 1990 — № 2 — С.35). Программу нужно вводить с адреса 1000. По окончании можно проверить правильность ввода программы, для этого, закончив ввод программы, нужно нажать клавишу «СТОП» и набрать следующие команды (то, что выводит на экран машина, подчеркнуто):

$1000АА = 001000
$1470ДД = 001470
$Х = 063625

$

Второй раз символы А и Д вводятся, чтобы проконтролировать правильность ввода адреса и длины массива. Если после ввода символа Х значение контрольной суммы отличается от 063625, программа была введена с ошибками. Для устранения ошибок повторить те же действия, что и при вводе программы, но если в текущей ячейке значение записано правильно, не переписывать его, а просто перейти к следующей ячейке, нажав «,». После исправления ошибок можно записать программу на магнитофон. Для этого набрать:

«СТОП»
$МЗ
НАЖМИТЕ КЛАВИШИ МАГНИТОФОНА
"ПУСК" И "ЗАПИСЬ"
АДРЕС = 1000

ДЛИНА = 1470
ИМЯ = «ЛАТ»SOS2
(файл записывается на магнитофон)
$

Следует иметь в виду, что при запуске программа сама себя модифицирует, поэтому запускать программу можно только после подсчета контрольной суммы и записи на магнитофон. Запуск программы осуществляется командой 1000G или S1000 из монитора. После запуска программа очищает экран и высвечивает за-

```
104014 012701 002034 005002 104020 104006 012701 002276 005002 104020
012737 001344 000004 004767 000314 012737 001336 000004 005701 100754
162701 040000 010167 001404 012702 040000 012703 003000 112223 077102
000425 012701 002445 005002 104020 012701 002466 012702 005020 104010
012700 000232 104016 005702 001404 005301 112721 000040 077203 012701
002460 104036 105737 000056 001003 112767 000232 001172 012701 002356
005002 104020 104006 042700 000240 020027 000122 001001 000673 020027
000105 001002 104014 000000 020027 000127 001001 000721 020027 000126
001355 012701 003000 010103 066703 001210 012702 002777 112700 000014
104016 020103 103022 121127 000040 103413 121127 000240 103003 121127
000177 101005 112100 104016 077216 104006 000753 005201 012700 000177
000770 012706 001000 000702 012706 001000 000632 005000 005001 012702
000200 012703 177716 012705 000040 005200 005301 030513 001374 000240
005200 005201 030513 001774 000240 005300 005201 030513 001374 000240
005300 005301 030513 001774 077224 005037 000300 005700 100001 005100
005701 100001 005101 020001 101402 005237 000300 004767 000234 012705
000040 012703 177716 005000 005001 012702 000140 005200 005200 030513
001375 005200 030513 001775 005201 030513 001375 005201 030513 001775
077216 020001 103401 010100 012702 000006 006200 077202 010037 000314
012737 000001 000304 012702 035000 012701 040000 012704 000010 012700
077760 012720 000777 077403 012700 077760 005004 005204 030513 001375
005204 030513 001775 023704 000314 101366 005004 005204 030513 001375
005204 030513 001775 160420 100411 042700 100000 052700 077760 030513
001376 030513 001776 000756 004737 117336 000207 012701 002010 012702
000005 005005 012704 000400 105737 000300 001003 005004 012705 000400
042771 000400 000000 050531 042771 000400 000000 050431 077211 000207
001524 001532 001540 001546 001642 001650 001666 001674 001714 001720
125232 115665 132665 132665 123665 047523 031123 132647 132665 132665
132633 012643 170267 147722 151307 146701 140715 157040 142724 144716
020321 140706 146312 153717 151440 147440 144733 145702 146701 133711
133425 067503 074560 064562 064147 020164 074542 160440 166456 167056
142301 153305 147311 030440 027061 027067 034461 030071 012667 132646
132633 132665 132665 132665 132665 132665 132665 132665 115665 134665
012425 146344 020321 140716 140736 140714 157040 142724 144716 020321
140716 146726 152311 020305 140314 152702 020300 146313 153701 155711
000325 015014 015032 146344 020321 145717 147317 140736 144716 020321
152336 147305 150711 147040 153301 144715 142724 145440 140714 144727
152733 036040 172363 170357 000076 011022 165634 166757 167341 174744
116072 053040 170055 147722 146723 152317 026322 053440 175055 150301
151711 026330 051040 171055 151705 140724 152322 020054 026505 154767
147710 114704 011000 146751 020321 020072 115231 000000 000002 003000
000000 001242
```

ставку. Для того чтобы начать чтение, включите магнитофон, дождитесь конца настроечной последовательности (монотонный звук в начале файла) и нажмите любую клавишу на клавиатуре БК. При нормальном чтении экран должен в такт со звуком начать заполняться неравномерными полосами из цветных точек. По окончании звука читающегося файла нажмите клавишу «СТОП», при этом в верхней строке экрана появится меню следующего вида:

V-просмотр, W-запись, R-рестарт, E-выход.

В режиме меню можно:

нажав клавишу «V» (на любом регистре) просмотреть на экране считанный текстовый файл (управляющие символы выводятся на экран в виде знаков забоя (закрашенное знако-место) для просмотра следующего экрана текста нужно нажать любую клавишу, для выхода в меню — клавишу «СТОП».

нажав «W», записать считанный файл на магнитофон, при этом в ответ на появившуюся в верхней строке подсказку: «Имя ?» нужно набрать имя файла и нажать «ВВОД».

нажав «R», стереть из памяти текущий файл и приготовиться к чтению следующего.

нажав «E», закончить работу с программой и выйти в монитор БК.

Можно рекомендовать следующую последовательность работы с программой SOS2:

1. Прочитать файл, визуально контролируя на экране отсутствие сбоев.

2. Командой V просмотреть файл на экране, если файл не содержит осмысленного текста, попробовать прочитать его еще раз, нажав «СТОП» и «R».

3. Командой «W» записать файл на магнитофон.

4. С помощью отладчика или текстового редактора откорректировать полученный файл.

(Окончание. Начало на с. 24)

компьютер "сходит с ума". Вирус "Воскресенье" не менее остроумен. Если он попал в программное обеспечение компьютера, в первое же воскресенье на экране появляются слова: "Сегодня воскресенье! Что ж ты все работаешь? Давай развлечемся!" Затем компьютер останавливается...

(ТАСС, 18 июля)

В 1989 г. выявлены два компьютерных вируса. Первый из них получил обозначение 1813 в соответствии с установившимся среди специалистов обычаем характеризовать вирус числом байтов, которые он добавляет к некоторым файлам (часто это число соответствует длине программы компьютерного вируса). Вирус 1813 уничтожает файлы с расширениями .EXE и .COM по определенным "несчастливым" дням. Впервые этот вирус был обнаружен в пятницу 13 января 1989 г., и впоследствии выяснилось, что он не особенно опасен, так как "затертые" файлы можно восстанавливать с помощью некоторых пакетов программ. Сейчас рынок наводнен программами обнаружения вируса 1813.

Наиболее простой способ предотвращения вредных последствий действия вируса 1813 — переключение системного календаря таким образом, чтобы он никогда не показывал 13-е число.

Большую озабоченность вызывает обнаруженный в США летом 1989 г. вирус "Дейтакрайм", который портит файлы с расширениями .EXE и .COM и таблицу распределения файлов .(FAT). Вирус "Дейтакрайм" — это "мина замедленного действия", находящаяся в "спящем" состоянии до определенного момента — он форматирует часть жесткого диска каждый день между 13 октября и 31 декабря, а также копирует сам себя в файлы .EXE и .COM. Вторая версия этого вируса форматирует часть жесткого диска каждый день, кроме 12 октября и любого числа, приходящегося на понедельник.

Computer Weekly, (Англия), № 1185, 12 октября 1989 г., стр.3

Юрий Волынский,
(МФН "Искатель",
г.Симферополь)

ЗАДАЧА О ПЕРЕСЕЧЕНИИ ОТРЕЗКОВ

Ставится следующая задача. На оси OX с помощью массивов L и R левых и правых границ задается множество I, состоящее из N-отрезков. Требуется построить алгоритм, определяющий, имеет ли место пересечение по меньшей мере двух отрезков множества I (существуют ли в I отрезки, имеющие общую часть).

Одним из подходов к решению задачи является следующий:

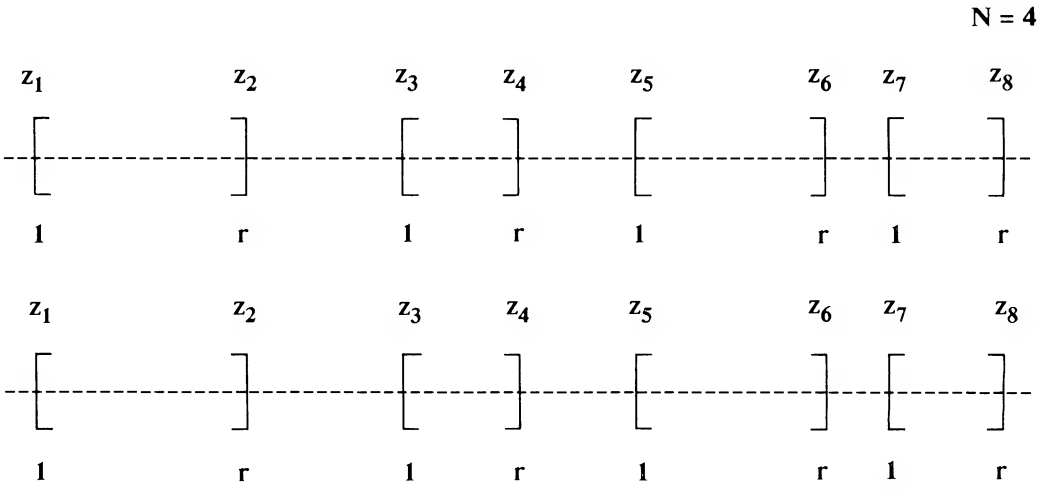
1. Слить массивы L и R в единый массив Z, состоящий из 2N-элементов.

2. Упорядочить Z по неубыванию, снабдив каждый его элемент признаком "l" (левая граница) или "r" (правая граница).

3. Проверить, является ли строка S признаков "l" и "r", построенная в п.2, повторением пары "lr" N раз. Если да, то пересечение не имеет места, в противном случае имеет.

Приведенный выше алгоритм реализован на языке Turbo Pascal. Для упорядочивания массива Z и строки S используется метод Шелла.

```
PROGRAM INTERSECTION_1D;
  Uses Crt;
  Const N  = 16;
        N2 = 32;
  Type Natural   = 0..MaxInt;
       RealArray = Array[1..N2] of Real;
  Var z : RealArray;
      s : String ;
    i,k : Natural ;
  Procedure Shell_Sort (Var A: RealArray;
                        Var W: String ;
                            N: Natural);
  Var X : Char ;
      Y : Real ;
   Dist : Natural;
    i,j : Natural;
  Begin
      Dist : = N div 2;
    While Dist > = 1
      Do
       Begin
        for i : = dist + 1 To N
          Do
           Begin
              Y : = A[i] ;
              X : = W[i] ;
               j : = i - Dist ;
```



```
            While (A[j] > Y) and (i > = 1)
              Do {INSERTION SORTING}
                Begin
                    A [j + Dist] : = A[j] ;
                    W [j + Dist] : = W[j] ;
                              j : = j - Dist ;
                End;
              W[j + Dist] : = X;
              A[j + Dist] : = Y;
            End;
          Dist : = Dist div 2 ;
        End;
    End;
BEGIN
  ClrScr;
  Writeln ('ЗАДАЧА О ПЕРЕСЕЧЕНИЯХ ОТРЕЗ-
           КОВ');
  Writeln;
  Write ('СКОЛЬКО ОТРЕЗКОВ?');
  ReadLn(K);
  Writeln;
  S: = '';
  For i : = 1 to K Do
    Begin
      Write ('L,R = '); Read (Z[i],Z[i + k]);
                        S : = 'L' + S + 'R'
    End;
    Shell_Sort(Z,S,2*K);
    Writeln;
    Writeln (S);
    Writeln;
    Writeln ((Pos('LL',S) = 0) and (Pos('RR',S) = 0) );
  END.
```

КОММЕНТАРИЙ СПЕЦИАЛИСТА

Задача о пересечении отрезков является одной из основных в научной дисциплине, которая называется вычислительной геометрией. Являясь базовой, эта задача широко используется при решении более сложных геометрических задач.

Поэтому очень важно иметь эффективный (наиболее быстрый) алгоритм, решающий поставленную задачу.

Использованный выше подход позволяет легко оценить сложность предложенного алгоритма, так как известно, что метод Шелла в сочетании с поиском подстроки в строке требует 0(NlogN) временных затрат. Поэтому приведенное решение лучше очевидного алгоритма попарного анализа отрезков, который имеет сложность 0(N^2).

Предложенную программу можно несколько упростить, выполняя поиск в S только подстроки "ll", так как из существования в S "ll" следует существование в ней "rr" и обратно.

Решение задачи иллюстрирует на элементарном уровне важную идею использования анализа слов для структурного распознавания образов. Геометрический образ, заданный множеством отрезков, отображается в другую предметную область и представляется в виде слова в двоичном алфавите A = {l,r}. Полученное слово в алфавите A является грамматической моделью геометрического образа. Анализируя грамматическую модель средствами символьной обработки, мы получаем ответ на вопрос, касающийся свойств исследуемого объекта.

Во всей полноте эта задача раскрывается при переходе к большим размерностям. Интересно, что алгоритм, распознающий пересечение отрезков плоскости, можно вычислить, как и в одномерном случае, за время 0(NlogN).

И.А.Переход

Компьютер и фирма-изготовитель*	Цена	Характеристики				Оценки								
Совместимые с IBM PC/XT	Базовый комплект**	Дисковод для гибких дисков	Жесткий диск	ОЗУ	Монитор	Клавиатура	Дисплей	Центральный блок	Конструкция	Документация	Прилагаемые программы	Производительность	Обслуживание	Комплексная оценка
Amstrad PC1640 Amstrad U.S.A.	$899	1x360K	20MB	640K	EGA color	2	4	3	3	3	4	4	2	3
ARC Turbo Model 10 American Research Corp.	$1,509	2x360K	20MB	640K	TTL mono	3	3	3	3	2	2	3	3	3
Beltron XT Turbo/20 Beltron Computer Corp.	$1,100	1x360K	20MB	640K	TTL mono	3	3	3	2	2	1	4	2	3
Commodore Colt Commodore Business Machines Inc.	$1,399.90	2x360K	-	640K	TTL/analog/ composite	2	4	3	4	3	4	3	3	3
Compuadd Standard Turbo/10 Compuadd Corp.	$649	1x360K	20MB	640K	TTL mono	4	3	3	3	3	1	4	3	3
Cordata WPC Cordata Technologies Inc.	$995	2x360K	-	768K	TTL mono	3	3	3	2	4	4	3	2	3
Delta Gold Elite Delta Computer Corp.	$1,195	2x360K	-	512K	TTL mono	5	4	4	4	5	4	4	4	4
Epson Apex Epson America Inc.	$899.99	2x360K	-	512K	CGA color	4	2	3	2	3	4	3	3	2
Hitech SAM 2001 Hitech International Inc.	$900	1x360K	-	640K	TTL mono	3	3	3	3	3	3	4	3	3
IBM Model 25 IBM Corp.	$1,350	2x360K	-	640K	Analog color	4	4	4	4	2	2	3	3	3
Innovation Model 1010XT Innovation Computer Corp.	$1,294	2x360K	20MB	640K	TTL mono	3	3	3	3	1	1	3	3	3
Laser Compact XT Laser Computers Inc.	$599	1x360K	-	512K	TTL mono	2	3	2	3	3	1	4	2	3

По пятибалльной системе

В течение двух последних лет лаборатория Clone Lab, созданная при журнале PC Resource, всесторонне протестировала десятки ПК, относящихся по меньшей мере к трем разным классам. Результаты этих исследований сведены в приведенную ниже таблицу, которая поможет вам быстро и правильно вы-

Leading Edge Model D Leading Edge Hardware Products Inc.	$995	2x360K	-	512K	TTL mono	4	3	4	3	4	4	3	4	4
Magitronic T800 Magitronic Technology Inc.	$784	1x360K	20MB	640K	TTL mono	2	3	3	3	2	1	4	3	3
Maxar 8ßS Maxar Computers	$1,069	2x360K	-	768K	TTL mono	4	3	4	4	3	3	3	3	3
Northgate XTurbo Northgate Computer Systems	$1,259	2x360K	20MB	640K	TTL mono	4	3	4	3	2	2	4	4	3
PC Popular Model 20 Blue Chip Electronics Inc.	$799.99	1x360K	20MB	640K	CGA color	3	4	2	3	4	4	3	4	3
Tandon PCX-20 Tandon Corp.	$1,499	1x360K	20MB	256K	TTL mono	3	3	3	3	4	3	2	3	3
Tandy 1000 HX Tandy Corp.	$699	2x720K	-	640K	CGA color	2	4	3	3	3	4	3	3	3
The Clone Clone Computers Inc.	$749	1x360K	20MB	640K	Analog color	3	3	4	3	2	4	3	4	3
Ultra-Comp Turbo 10 Ultra-Comp	$739	2x360K	-	640K	TTL mono	3	3	3	3	1	1	4	3	3
Vendex Turbo-888-XT Vendex Pacific Inc.	$995	2x360K	-	512K	CGA color	3	4	3	4	5	5	4	4	4
Xtra Professional Series 300 Xtra Business Systems	$609	1x720K, 1x360K	20MB	768K	TTL mono	3	3	4	4	2	1	4	3	3
Zenith Eazy PC Model EZ-20 Zenith Data Systems	$1,699	1x720K	20MB	512K	TTL mono	4	4	3	1	3	3	3	3	3
Zenith Z-159 Zenith Data Systems	$1,599	1x360K	20MB	512K	TTL mono	4	5	4	4	4	3	4	3	4
Совместимые с IBM PC/AT														
Amdek System/286A Amdek Corp.	$2,595	1x1.2MB	40MB	1MB	EGA color	4	3	4	4	3	4	5	3	4
AT Rose Hill Model 1700 Rose Hill Systems	$1,325	1x1.2MB	40MB	1MB	EGA color	3	4	3	3	3	2	5	3	3
Clone 286 Clone Computers	$1,499	1x1.2MB	40MB	1MB	TTL mono	2	3	3	3	2	3	4	4	3
Cordata 4210 Cordata Technologies Inc.	$1,380	2x360K	-	640K	TTl mono	2	4	4	3	3	3	3	2	3

брать компьютер, наиболее полно отвечающий вашим потребностям и возможностям. Оценки выставлены по пятибалльной системе. Оценка 1 означает, что изделие или его обслуживание неприемлемо, 2 — ниже среднего, 3 — соответствует описанию, 4 — выше среднего, 5 — превосходно.

PC Resource. — 1989. — January, см. также ПК-ЭКСПРЕСС. — 1989. — № 1

Компьютер и фирма-изготовитель*	Цена	Характеристики				Оценки								
Совместимые с IBM PC/XT	Базовый комплект**	Дисковод для гибких дисков	Жесткий диск	ОЗУ	Монитор	Клавиатура	Дисплей	Центральный блок	Конструкция	Документация	Прилагаемые программы	Производительность	Обслуживание	Комплексная оценка
Dell System 220 Dell Computer Corp.	$2,299	1x1.44MB	40MB	1MB	VGA color	4	3	5	4	5	2	5	5	4
Heritage 286/12 Computer Components Corp.	$1,349	1x1.2MB	40MB	1MB	color multiscan	2	4	3	4	3	3	5	3	3
Hyundai Super-286C Hyundai Electronics America	$1,645	1x360K, 1x1.2MB	30MB	640K	CGA color	3	4	3	4	3	3	4	4	4
Leading Edge Model D2 Leading Edge Hardware Products Inc.	$1,495	1x1.2MB	65MB	640K	TTL mono	4	3	4	4	4	4	4	4	4
Micro 1 286 + Power-12 Micro 1	$1,395	1x1.2MB	44MB	1MB	TTL mono	3	4	3	4	2	2	5	3	4
Mitsubishi MP286 Mitsubishi Electronics America Inc.	$1,895	1x1.2MB	40MB	640K	EGA color	4	4	4	3	4	3	4	3	4
Proteus-286E Proteus Technology Corp.	$1,513	1x1.2MB	20MB	1MB	TTL mono	3	3	3	3	4	2	3	5	3
Proteus-286/20 Proteus Technology Corp.	$1,850	1x1,2MB	40MB	1MB	EGA color	3	4	3	3	4	2	5	5	3
Sysgen Prosystem Sysgen Inc.	$2,395	1x1.2MB 1x1.44MB	40MB	640K	EGA color	4	4	4	4	2	2	4	4	4
Uniq AT-Turbo 286 Unique Technology Inc.	$1,260	1x1.2MB	40MB	1MB	EGA color	4	4	3	3	2	1	5	4	3
Vector Excalibur 286 Vector Computer Corp.	$2,295	1x1.2MB	65MB	512K	EGA color	4	2	3	4	2	3	5	4	3
Wyse PC 286 Model 2108 Wyse Technology	$1,799	1x1.2MB	20MB	512K	EGA color	4	4	3	4	3	4	3	3	4

мерческие секреты, и не знают, как проследить несанкционированные обращения к компьютеру. Много дел было проиграно из-за того, что полицейский, занимавшийся дознанием, не знал, как сохранить доказательства, обнаруженные на компьютере. Не раз полицейский офицер, страдающий компьютерной безграмотностью, позволял подозреваемому подключиться к компьютеру и уничтожить важнейшие доказательства. Полицейские стараются держаться подальше от компьютерных преступлений, так как расследование их чрезвычайно сложно.

Многие из этих проблем затрагивают и следователей прокуратуры. Большинство их не обладают нужным уровнем компьютерной грамотности, а навыки, необходимые для расследования обычных преступлений, не всегда переносимы на область компьютерной преступности.

Таким образом, основная часть компьютерных преступлений остается безнаказанной.

Проблемой компьютерной преступности следует заниматься немедленно, поскольку это растущая угроза экономике. В регионах, насыщенных предприятиями наукоемких отраслей, следует создать специальные подразделения, единственным назначением которых

На базе микропроцессора 80386														
Acer Model 1100 Acer Technologies Corp.	$3,495	1x1.2MB	40MB	3MB	EGA color	4	4	3	3	4	3	3	4	4
Compaq Deskpro 386/20 Compaq Computer Corp.	$7,499	1x1.2MB	130MB	5MB	VGA color	3	3	3	4	4	2	5	3	4
IBM PS/2 Model 80 IBM Corp.	$6,995	1x1.44MB	40MB	4MB	Analog color	4	5	5	5	2	2	4	3	4
Tandy 4000 Tandy Corp.	$2,599	1x1.44MB	40MB	3MB	EGA color	2	4	3	3	3	3	3	3	3
Портативные														
IBM PC Convertible Model 3 IBM Corp.	$1,695	2x720K	-	640K	backlit LCD	4	4	3	4	4	2			
NEC Multispeed EL NEC Home Elkctronics Inc.	$2,295.	2x720K	-	640K	backlit LCD	4	3	3	3	4	5	5	3	4
Sharp PC-4502 Sharp Electronics Corp.	$1,795	2x720K	-	640K	backlit LCD	2	3	3	3	2	3	3	3	3
Tandy 1400 LT Tandy Corp.	$1,799	2x720K	-	768K	backlit LCD	3	3	4	3	3	4	3	3	3

* В таблицу включены только ПК, выпускаемые до сих пор.

** Цена базового комплекта периодически изменяется.

(Впервые опубликовано в ПК-экспресс № 1 1989)

Компьютерная преступность

То, что компьютеры стали инструментами антиобщественного поведения, вряд ли удивительно. Вызывает удивление то, что очень мало делается для того, чтобы остановить компьютерную преступность. Первая линия обороны против компьютерных преступников — меры безопасности, принимаемые на уровне системы, оказывается одновременно самой слабой. Компьютеры уязвимы по своей сути.

Мошенники могут легко перенести информацию с универсальной ЭВМ на дискету и вынести ее с предприятия или послать себе домой по почте. Поскольку служащие нуждаются в доступе к файлам их коллег, они часто знают еще несколько паролей, кроме собственного. При этом мошенничество или кража происходят, не оставляя в "контрольных журналах" компьютерной системы следа, необходимого для идентификации преступника.

Решение, видимо, заключается в том, чтобы ограничить доступ к компьютеру. Но ужесточение мер безопасности отражается на психологическом состоянии сотрудников и производительности труда.

Большинство полицейских офицеров не являются специалистами в области компьютеров, не могут правильно оценить заявление о том, что подозреваемый похитил компьютерную информацию, должно быть расследование компьютерных преступлений. Второй шаг — приведение наказания в соответствие со степенью опасности преступления.

В Англии выработаны рекомендации относительно дополнения уголовного законодательства для борьбы с компьютерными преступлениями. Рекомендуется считать преступлениями:

— несанкционированный доступ в компьютерную систему как для забавы, так и с целью нарушения ее работы и наказывать за это тюремным заключением сроком на три месяца;

— несанкционированный доступ в компьютерную систему с намерением совершить серьезное преступление и наказывать за это тюремным заключением на срок до пяти лет;

— создание и распространение компьютерных вирусов, т. е. программ, преднамеренно и без санкции соответствующих лиц изменяющих хранящиеся в компьютерах данные или программы, и наказывать за это заключением в тюрьму на срок до пяти лет.

Texnology Review (США), т.93, № 2, 1990 г., стр.34-40.
Computer Weekly (Англия), № 1185, 12 октября 1989 г., стр.3.

3-40 **Защита** информации. — М.: Знание, 1990. — 48 с. — (Новое в жизни, науке, технике. Сер. "Вычислительная техника и ее применение"; № 9).

ISBN 5-07-001511-7

20 к.

В выпуске рассмотрены некоторые аспекты многогранной проблемы защиты информации в вычислительных системах от несанкционированного доступа, кражи, вирусов и т.д.

Брошюра рассчитана на широкий круг читателей.

2404040000 **ББК 32.97**

ТЕМА *СЛЕДУЮЩЕГО* **НОМЕРА:**

РАДИО-ЭЛЕКТРОНИКА И СВЯЗЬ

Эволюция технологий или новая история времени

***ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА* И ЕЁ ПРИМЕНЕНИЕ**

Экспертные системы

МАТЕМАТИКА КИБЕРНЕТИКА

Машинная геометрия и графика

Научно-популярное издание

ЗАЩИТА ИНФОРМАЦИИ

Гл.отраслевой редактор *Г. Г. Карвовский*
Редактор *Б. М. Васильев*
Мл.редактор *Н. А. Васильева*
Художник *В. Н. Конюхов*
Худож.редактор *И. А. Емельянова*
Техн.редактор *Т. В. Луговская*
Корректор *В. И. Гуляева*

ИБ № 11193

Подписано к печати 2.08.90. Формат бумаги 70×100$^{1}/_{16}$. Бумага офсетная. Печать офсетная. Усл. печ. л. 3,90. Усл. кр.-отт. 8,45. Уч.-изд. л. 4,0. Тираж 72 347 экз. Заказ 1419. Цена 20 коп. Издательство «Знание». 101835, ГСП, Москва, Центр, проезд Серова, д. 4. Индекс заказа 904709. Отпечатано с оригинал-макета издательства «Знание» на ордена Трудового Красного Знамени Тверском полиграфическом комбинате Государственного комитета СССР по печати. 170024, г. Тверь, пр. Ленина, 5.

Цена 20 коп.

Индекс 70195

Адрес подписчика:

10-32

Издательство «Знание»

Подписная научно-популярная серия

ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ЕЕ ПРИМЕНЕНИЕ

"...вопрос о технике стал вопросом о судьбе человека и судьбе культуры"

Н. Бердяев

Даже увеличение мощности компьютера в миллион раз не поколеблет того факта, что большинство задач невозможно решить только за счет "грубой силы". Они требуют разумного применения знаний, позволяющих ограничить поиск

Дуглас Б. Лент

Наш адрес:
СССР,
Москва,
Центр,
проезд
Серова, 4